AN ABSTRACT OF THE THESIS OF

YOUNG HYUN PAIK for the MASTER OF SCIENCE
(Name) (Degree)

in MATHEMATICS presented on April 10, 1969
(Major) (Date)

Title: ON THE CALCULATION OF THE COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

Abstract approved Redacted for Privacy
Harry E. Goheen

In this paper, we are concerned with the general notion on the cyclotomic polynomial and a general procedure for obtaining its coefficients.

The cyclotomic polynomial is defined as the products of the linear equations whose roots are all primitive n^{th} roots of unity and one of its most striking properties is the smallness of its coefficients.

The author treats results of previous works and general concepts of it in Chapter 1 through 4. In the last chapter, the author, using Hölder's formula and Newton's identities, gives a procedure in detail for obtaining recursively all the coefficients of the cyclotomic polynomial $Q_n(x)$ for $n = 105$ and $n = 595$ and illustrates them in tables.

On the Calculations of the Coefficients of Cyclotomic Polynomials

by

Young Hyun Paik

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Master of Science

June 1969

APPROVED:

Redacted for Privacy

Professor of Mathematics

in charge of major

Redacted for Privacy

Acting Chairman of Department of Mathematics

Redacted for Privacy

Dean of Graduate School

Date thesis is presented April 10, 1969

Typed by Muriel Davis for Young Hyun Paik

ACKNOWLEDGMENT

The author wishes to express his sincere appreciation to Dr. Harry E. Goheen for his helpful guidance and encouragement and to Dr. Robert D. Stalley for his helpfulness during this study.

A word of thanks is extended to Mr. Junpei Sekino and Mr. Soo Il Kang for helpful discussions.

Special acknowledgment is given to his father and wife, Jung Ja, for their patience, support and sacrifice, willingly offered, which made it possible for him to complete this work.

TABLE OF CONTENTS

LIST OF TABLES

ON THE CALCULATION OF THE COEFFICIENTS OF CYCLOTOMIC POLYNOMIALS

CHAPTER 1. INTRODUCTION

§1. Purpose of This Paper

The aim of this work is to derive a general procedure for finding recursively the coefficients of any cyclotomic polynomial.

Much has been done on the properties of the coefficients of the cyclotomic polynomial but there has been little interest in obtaining general formulas to get coefficients of any cyclotomic polynomial. The methods suggested are very theoretical and complicated in actual calculations.

The author tried to find a simple formula using results of previous works, especially Hölder's formula simplifying Ramanujan sum and Newton's identities. Rather than formula this paper presents a well-defined algorithm.

Chapter 1 gives the results of previous works. General ideas and some important theorems on the coefficients of the cyclotomic polynomial are developed in Chapter 2 through 4. In Chapter 5 the author explains in detail a procedure for obtaining the coefficients and its application for the cases $n = 105$ and $n = 595$.

Throughout this paper the author uses symbol $Q_n(x)$ for the cyclotomic polynomial.

§2. The Results of Previous Works

There have been published many important and interesting results of investigations on the coefficients of the cyclotomic polynomial since the latter half of the 19th century. Here we shall review some of them in chronological order.

A. Migotti in 1883 showed that the coefficients of $Q_n(x)$ are all ± 1 or 0 for n, a product of two primes but noted that the coefficient of X^7 in $Q_{105}(x)$ is -2. This result is quoted from [12].

A. S. Bang in 1895 [1] proved that no coefficients of $Q_n(x)$ for $n = pqr$, $(p < q < r$; odd primes) exceeds $p-1$ and also proved that the coefficients of $Q_n(x)$ are ± 1 and 0 for a product of the first powers of two distinct primes.

I. Schur in 1931 proved that there exist cyclotomic polynomials with coefficients arbitrarily large in absolute value. This again is quoted from reference [12].

Bungers in 1934 proved the same theorem as Schur's under the assumption that there exist infinitely many prime pairs for n a product of three primes. This also is quoted from [12].

E. Lehmer in 1936 [12] modified Bungers' proof so as to eliminate his unproved assumption of the existence of infinitely many prime pairs.

O. Hőlder in 1936 [9] showed that if $C_n(k)$ denotes the (Ramanujan) sum of the k^{th} powers of the primitive n^{th} roots of unity then

$$C_n(k) = \phi(n)\frac{\mu(n/d)}{\phi(n/d)}$$

where d is the greatest common divisor (n,k) of n and k.

J. E. Eaton in 1939 [5] gave formulas for calculation of the coefficients of the cyclotomic polynomial by means of combinatorial methods. Special properties of the coefficients such as magnitude and increase, which in later times have been considered, Eaton couldn't obtain by his method.

P. Erdős in 1946 [6] proved that if A_n denotes the largest coefficient (in absolute value) of the n^{th} cyclotomic polynomial, then for infinitely many n

$$A_n > \exp\{c_1(\log n)^{4/3}\} .$$

He also conjectured that a much stronger statement may be true, namely that

$$(A)\quad A_n > \exp\{n^{(c_{13}/\log\log n)}\}$$

holds for some c_{13} and infinitely many n, but pointed out that this would be a best result since

$$(B)\quad A_n < \exp\{n^{(c_{14}/\log\log n)}\}$$

for some c_{14} and all n.

P. T. Bateman in 1949 [2] gave the short proof of (b) of Erdős' paper just quoted.

E. Gagliardo in 1953 [7] proved the formula

$$S_k(n) = \mu\left(\frac{n}{(n, k)}\right)\phi(n)/\phi\left(\frac{n}{(n, k)}\right)$$

which is due to Hölder. Hölder's earlier work is not mentioned and his methods are not the same.

G. S. Kajandzidis in 1963 [11] obtained a general formula for the coefficients of the cyclotomic polynomial

$$\phi_N(x) = \prod_{d\delta=N} (1-x^d)^{\mu(\delta)} = 1 + a_1 x + \cdots + a_M x^M + \cdots .$$

Utilizing the results of E. Gagliardo, he proved that

$$a_M = \sum_{\Sigma i a_i = M} \frac{\left(-\frac{S_1}{1}\right)^{a_1}\left(-\frac{S_2}{2}\right)^{a_2} \cdots \left(-\frac{S_N}{N}\right)^{a_N}}{a_1!\, a_2! \cdots a_N!}$$

where $N = p_1 \cdots p_\nu$ with $p_1 < \cdots < p_\nu$ and the summation is taken over all non-negative integral solutions of the Diophantine equation $1a_1 + 2a_2 + \cdots + Na_N = M$, and S_N stands for the sum of the n^{th} powers of the roots of $\phi_N(x)$.

He also found a second general formula and reobtained Migotti's result for $N = pq$ ($p < q$, primes).

Sister Marion Beiter in 1964 [3] proved that if

$$F_{pq}(x) = \sum_{n=0}^{\phi(pq)} c_n x^n$$

then

$$c_n = \begin{cases} (-1)^{\delta} & \text{if } n \text{ has the form explained below,} \\ 0 & \text{otherwise} \end{cases}$$

The special form of n is that $n = \alpha q + \beta p + \delta$ where α, β are non-negative integers and δ is 0 or 1 and this representation is unique. She also determined the middle coefficient c_n where $n = \phi(pq)/2$.

L. Carlitz in 1966 [4] determined the number of nonzero terms in $Q_{pq}(x)$, p and q distinct primes.

CHAPTER 2. GENERAL THEORY

§1. Roots of Unity[1/]

We are concerned with the equation

$$x^n = 1$$

and the polynomial $Q_n(x)$ of degree $\phi(n)$, Euler's ϕ-function of n, which has as roots the primitive n^{th} roots of unity, in case of a field of characteristic prime to n or of characteristic 0.

Definition 2.1. By a n^{th} root of unity we shall mean a root of the polynomial

$$f(x) = x^n - 1$$

in any commutative extension field.

Proposition 2.2. The n^{th} roots of unity in a field form an Abelian group under multiplication.

Proof. If $\alpha^n = 1$ and $\beta^n = 1$, then $(\frac{\alpha}{\beta})^n = 1$, from which the group property follows. It is obvious that the group is an Abelian group.

The order k of a group element α is a divisor of n, since we must have $\alpha^n = 1$ and if $n = qk + r$ for $k \leq n$.

[1/] This is a summary of the pertinent materials in [8] and [16].

$a^n = a^{qk+r} = (a^k)^q \cdot a^r = 1$, but $(a^k)^q = 1$ we must have $r=0$. Thus k divides n.

The splitting field K of $f(x)$ is called the field of the n^{th} roots of unity over the prime field Π. The polynomial $f(x)$ factors into linear factors which are all different from each other; for the derivative

$$f'(x) = nx^{n-1}$$

vanishes only when $x=0$, since n is not divisible by the characteristic and therefore has no root in common with $f(x)$. Thus there are exactly n n^{th} roots of unity in K.

Definition 2.3. If the order of a root of unity is exactly n, it will be called a primitive n^{th} root of unity.

Proposition 2.4. The group of the n^{th} roots of unity is cyclic and is generated by every primitive n^{th} root of unity ξ.

To prove this, we shall use the following lemmas and a theorem.

Lemma 2.5. Let G be a finite Abelian group enjoying the property that the relation $x^n = e$ is satisfied by at most n elements of G, for every integer n. Then G is a cyclic group.

Proof. If the order of G is a power of some prime number q then the result is true. For, suppose that $a \in G$ is an element

whose order is as large as possible; since its order must divide the order of G, it is q^r for some integer r. We do not yet know that q^r is the order of G, but the elements $e, a, a^2, \cdots, a^{q^r-1}$ give us q^r distinct solutions of the equation $x^{q^r}=e$.

Now suppose $b \in G$ and its order is q^s where $s \leq r$, hence $b^{q^r}=(b^{q^s})^{q^{r-s}}=e$, i.e., b is a solution to the equation $x^{q^r}=e$. Since the only solutions in G of this equation are the powers of a, b is a power of a, G is of order q^r and G is cyclic.

The general finite Abelian group G can be realized as $G=S_{q_1} S_{q_2} \cdots S_{q_k}$ where the q_i are the distinct prime divisors of $O(G)$ the order of G, and where the S_{q_i} are the Sylow subgroups of G. Moreover, every element $g \in G$ can be written in a unique way as $g=S_1 S_2 \cdots S_k$ where $s_i \in S_{q_i}$. Any solution of $x^n=e$ in S_{q_i} is one of $x^n=e$ in G so that each S_{q_i} inherits the hypothesis we have imposed on G. By the remarks of the first paragraph of the proof each S_{q_i} is a cyclic group; let a_i be a generator of S_{q_i}. We claim that $c=a_1 a_2 \cdots a_k$ is a cyclic generator of G. To verify this all we must do is to prove that $O(G)$ divides m, the order of c. Since $c^m=e$, we have that $a_1^m a_2^m \cdots a_k^m=e$. By the uniqueness of representation of an element of G as a product of elements in the S_{q_i}, we conclude that each $a_i^m=e$. Thus $O(S_{q_i}) \mid m$ for every i. Thus

$O(G) = (S_{q_1})O(S_{q_2})\cdots O(S_{q_k}) \mid m$. However, $m \mid O(G)$ and so $O(G)=m$.

This proves that G is cyclic. ∎

Lemma 2.5 has as an important consequence Lemma 2.6.

Lemma 2.6. Let K be a field and let G be a finite subgroup of the multiplicative group of nonzero elements of K. Then G is a cyclic group.

Proof. Since K is a field, any polynomial of degree n in $K[x]$ has at most n roots in K. Thus in particular, for any integer n, the polynomial $x^n - 1$ has at most n roots in K, and all the more so, at most n roots in G. The hypothesis of Lemma 2.5 is satisfied, so G is cyclic.

Even though the situation of a finite field is merely a special case of Lemma 2.6, it is of such wide-spread interest that we single it out as Theorem 2.7.

Theorem 2.7. The multiplicative group of nonzero elements of a finite field is cyclic.

Proof. Let F be a finite field. By merely applying Lemma 2.6 with $F=K$ and $G=$ the group of nonzero elements of F, the result drops out. ∎

Returning to Proposition 2.4, since the n^{th} roots of unity form a finite subgroup under multiplication, so by Theorem 2.7 this group is cyclic. Also any cyclic generator of the group must then be a primitive n^{th} root of unity. This proves Proposition 2.4. ∎

We shall now prove that the number of primitive n^{th} roots of unity is $\phi(n)$,[2] the number of elements of order n in a cyclic group of order n.

First, if n is a power of a prime number, $n=p^t$, all p^t powers of ξ, excepting the p^{t-1} powers of ξ^p are elements of order n. Hence we have

$$\phi(p^t) = p^t - p^{t-1} = p^{t-1}(p-1) = p^t\left(1-\frac{1}{p}\right). \tag{2.1.1}$$

Secondly, if n is decomposed into two relatively prime factors $n=rs$, every element of order n is uniquely representable as the product of an element of order r by an element of order s and, conversely, every such product is an element of order n. The elements of the r^{th} order belong to the cyclic group of order r generated by ξ^s; their number is $\phi(r)$. Similarly, the number of the elements of order s is $\phi(s)$; thus, for the number of the

---

[2] $\phi(n)$ is also the number of the natural numbers $\leq n$ relatively prime to n. $\phi(n)$ is called Euler's phi-function.

products we have

$$\phi(n) = \phi(r)\phi(s).$$

If $n = \prod_{i=1}^{m} p_i^{t_i}$ is the decomposition of n into relatively prime powers of prime numbers, the above formula yields by repeated application.

$$\phi(n) = \phi(p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}) = \phi(p_1^{t_1})\phi(p_2^{t_2}) \cdots \phi(p_m^{t_m});$$

hence by (2.1.1)

$$\phi(n) = p_1^{t_1-1}(p_1-1)p_2^{t_2-1}(p_2-1) \cdots p_m^{t_m-1}(p_m-1)$$

$$= n(1-\frac{1}{p_1})(1-\frac{1}{p_2}) \cdots (1-\frac{1}{p_m}).$$

Thus we have Proposition 2.8.

Proposition 2.8. The number of the primitive n^{th} roots of unity is

$$\phi(n) = n \cdot \prod_{i=1}^{m} (1-\frac{1}{p_i}).$$

We shall close this section with one additional remark.

The primitive n^{th} roots of unity are of absolute value 1 and being pairwise complex conjugates of modulus 1, the product of all the primitive n^{th} roots of unity is 1.

§2. Definition of the Cyclotomic Polynomial

The cyclotomic polynomial is defined as

$$(2.2.1) \qquad Q_n(x) = \prod_{(\ell, n)=1} (x - e^{\frac{2\pi i \ell}{n}})$$

in which the index ℓ ranges over the natural numbers prime to n and less than n and all $e^{\frac{2\pi i \ell}{n}}$ where $(\ell, n)=1$ are primitive n^{th} roots of unity, then

$$(2.2.2) \qquad Q_n(x) = 0$$

represents the equation of degree $\phi(n)$ which the primitive n^{th} roots of unity satisfy.

If $n > 2$, the roots fall into complex conjugate pairs, and hence the polynomial $Q_n(x)$ is always positive for real x.

Since $x^n - 1$ can be expressed as a product of linear factors, actually as

$$x^n - 1 = \prod(x - e^{\frac{2k\pi i}{n}}) \quad \text{where } k = 0, 1, 2, \cdots, n-1.$$

$$= (x-1)(x - e^{\frac{2\pi i}{n}}) \cdots (x - e^{\frac{2(n-1)\pi i}{n}}),$$

the definition of the primitive root shows that these factors can be grouped into distinct sets, each set being $Q_d(x)$ for some integer d dividing n, and $1 \leq d \leq n$. Thus we have

$$(2.2.3) \qquad x^n - 1 = \prod_{d \mid n} Q_d(x)$$

Taking logarithms yields the equation

$$\log(x^n - 1) = \log \prod_{d|n} Q_d(x) = \sum_{d|n} \log Q_d(x)$$

whence by the Möbius inversion formula[3] of elementary number theory follows

$$\log Q_n(x) = \sum_{d|n} \mu(d) \log(x^{\frac{n}{d}} - 1) \tag{2.2.4}$$

where $\mu(d)$ is the Möbius function[4] so that we have another expression of the cyclotomic polynomial

$$Q_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} \tag{2.2.5}$$

§3. The Properties of the Cyclotomic Polynomial

In the preceding sections, we have discussed about the n^{th} roots of unity and defined the cyclotomic polynomial, but we need to know further information about its properties to develop this work. Now we shall observe a couple of the elementary properties of it through

---

[3] Möbius inversion formula; If $F(n) = \sum_{d|n} f(d)$ for every positive integer n, then $f(n) = \sum_{d|n} \mu(d) F(n/d)$.

[4] Möbius function $\mu(n)$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 | n \text{ for some prime } p \\ (-1)^t & \text{if } n = p_1 p_2 \cdots p_t \text{ is a product of distinct primes.} \end{cases}$$

theorems and their proofs.

Theorem 2.9. The cyclotomic polynomial $Q_n(x)$ of order n is a monic polynomial of degree $\phi(n)$ with integer coefficients.

Proof. We employ induction. The theorem is true for $n=1, 2$.

Assume it to be true for all $Q_k(x)$, $k < n$. Now

$$x^n - 1 = Q_n(x) \cdot \prod_{\substack{d \mid n \\ d < n}} Q_d(x) = Q_n(x) \cdot G_n(x) . \tag{2.3.1}$$

But here, since $d < n$, $G_n(x)$ is a product of monic polynomials with integer coefficients, hence it is also monic with integer coefficients. Then

$$Q_n(x) = \frac{x^n - 1}{G_n(x)}$$

Long division produces only integer coefficients here because the divisor has highest coefficient 1.

Now as to the degree of $Q_n(x)$, if we assume the degree $\phi(d)$ for $Q_d(x)$, $d < n$, we have from (2.3.1), if v is the degree of $Q_n(x)$:

$$n = v + \sum_{\substack{d \mid n \\ d < n}} \phi(d) = v - \phi(n) + \sum_{d \mid n} \phi(d) .$$

Thus $v = \phi(n)$, in view of one of the theorems of elementary

number theory[5] (13, p. 36). ∎

Next we shall observe the irreducibility of $Q_n(x)$ in the rational field R_o. Before preceding with the argument we shall treat a useful lemma attributed Gauss concerned with primitive polynomials.

Definition 2.10. A nonconstant polynomial

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

where all a_i, $i = 0, 1, 2, \cdots, n$ are integers is said to be primitive if the greatest common divisor of all a_i is 1.

Lemma 2.11. (Gauss) If R_o is a U. F. D.[6] then a product of two primitive polynomials of $R_o[x]$ is again primitive.

Proof. Let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

be primitive in $R_o[x]$ and suppose that

$$f(x)g(x) = c_o + c_1x + \cdots + c_{n+m}x^{n+m}$$

is not primitive.

---

[5] Theorem; For $n \geq 1$, we have $\sum_{d|n} \phi(d) = n$

[6] U. F. D., unique factorization domain.

Then there exists a prime p such that $p \mid c_i$ for all i. Since $f(x)$ is primitive, p is not a factor of all a_i and we suppose that $a_{n'}$ is the last a_i not divisible by p. Similarly let $b_{m'}$ be the last b_i not divisible by p.

We now consider the coefficient

$$c_{m'+n'} = a_o b_{m'+n'} + a_1 b_{m'+n'-1} + \cdots + a_{n'-1} b_{m'+1} + a_{n'} b_{m'}$$

$$+ a_{n'+1} b_{m'-1} + \cdots + a_{n'+m'} b_o .$$

Since all the b_i before the term $a_{n'} b_{m'}$ are divisible by p and since all the a_j after this term are divisible by p and since $c_{m'+n'}$ is divisible by p, $p \mid a_{n'} b_{m'}$. But p is not a divisor of $a_{n'}$ or of $b_{m'}$ and this is a contradiction. ∎

Theorem 2.12. $Q_n(x)$ is irreducible in the rational field R_o.

Proof. (10, p. 112-113). Suppose that $Q_n(x) = h(x)k(x)$ where $h(x)$ is irreducible in $R_o[x]$ and deg $h(x) \geq 1$. By Gauss' lemma we may assume that $h(x)$ and $k(x)$ have integer coefficients and leading coefficients 1.

Let p be a prime integer such that $p \nmid n$ and let ξ be a root of $h(x)$. We shall show that ξ^p is a root of $h(x)$. Since $(p, n)=1$, ξ^p is a primitive n^{th} root of unity and, if ξ^p is not a root of $h(x)$ ξ^p is a root of $k(x)$; consequently ξ is a root

of $k(x^p)$. Since $h(x)$ is irreducible in $R_o[x]$ and has ξ as a root, $h(x) \mid k(x^p)$. It follows (as above) that $k(x^p) = h(x)\ell(x)$, where $\ell(x)$ has integer coefficients and leading coefficient 1. Also we have $x^n - 1 = Q_n(x)p(x) = h(x)k(x)p(x)$ and all of these polynomials have integer coefficients and leading coefficients 1.

We now pass to congruences modulo p or, what is the same thing, to relations in the polynomial ring $I_p[x]$. Then we obtain

$$x^n - \bar{1} = \bar{h}(x)\bar{k}(x)\bar{p}(x) \tag{2.3.2}$$

where in general, if $f(x) = a_o x^n + a_1 x^{n-1} + \cdots + a_n \in I[x]$, then $\bar{f}(x) = \bar{a}_o x^n + \bar{a}_1 x^{n+1} + \cdots + \bar{a}_n$, $\bar{a}_i = a_i + (p)$ in I_p. Similarly, we have $\bar{k}(x^p) = \bar{h}(x)\,\bar{\ell}(x)$.

On the other hand, using $\bar{a}^p = \bar{a}$ for every integer a, we see that

$$\bar{f}(x)^p = (\bar{a}_o x^n + \cdots + \bar{a}_n)^p = \bar{a}_o^p x^{pn} + \cdots + \bar{a}_n^p$$

$$= \bar{a}_o x^{pn} + \cdots + \bar{a}_n = \bar{f}(x^p)$$

for any polynomial $f(x)$. Hence $\bar{k}(x)^p = \bar{k}(x^p) = \bar{h}(x)\,\bar{\ell}(x)$ which implies that $(\bar{h}(x), \bar{k}(x)) \neq 1$. Then (2.3.2) shows that $x^n - \bar{1}$ has multiple roots in its splitting field over I_p. Since $p \nmid n$ this is impossible and so we have proved that ξ^p is a root of $h(x)$ for every prime p satisfying $p \nmid n$. A repetition of this process

shows that ξ^r is a root of $h(x)$ for every integer r prime to n. Since any primitive n^{th} root of unity has the form ξ^r, $(r, n) = 1$ we see that every primitive n^{th} root of unity is a root of $h(x)$. Hence $h(x) = Q_n(x)$ and $Q_n(x)$ is irreducible in $R_o[x]$. ∎

Finally we shall observe one more interesting theorem and close this chapter.

Theorem 2.13. The coefficients of the cyclotomic polynomial $Q_n(x)$ for $n > 1$ are symmetric to the midterm.

Proof. Let

$$Q_n(x) = x^{\phi(n)} + a_1 x^{\phi(n)-1} + \cdots + 1.$$

then $[Q_n(\frac{1}{x})]x^{\phi(n)}$ must be $Q_n(x)$ over again, for if ξ is a primitive root, so is $\frac{1}{\xi}$.

But

$$Q_n(\frac{1}{x})x^{\phi(n)} = x^{\phi(n)} + a_{\phi(n-1)}x^{\phi(n)-1} + \cdots + 1$$

Thus

$$a_{\phi(n)-i} = a_i \qquad i = 1, 2, \cdots, \phi(n).$$ ∎

CHAPTER 3. SOME IDENTITIES AND THEIR APPLICATIONS

§1. Some Identities and Their Proofs

From the definition of the cyclotomic polynomial

$$Q_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)} \tag{3.1.1}$$

we can derive a few useful and important identities. Here we shall make a list of these identities and give proofs of them.

Identity 3.1. If p is a prime

$$Q_p(x) = x^{p-1} + x^{p-2} + \cdots + 1.$$

Proof. By (3.1.1)

$$Q_p(x) = \prod_{d|p} (x^{p/d} - 1)^{\mu(d)}$$

$$= (x^p - 1)^{\mu(1)} (x-1)^{\mu(p)}$$

$$= (x^p - 1)(x-1)^{-1}$$

$$= \frac{(x^p - 1)}{(x-1)} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 \quad \blacksquare$$

Identity 3.2. If p is a prime and for an integer $r \geq 1$

$$Q_{p^r}(x) = Q_p(x^{p^{r-1}})$$

Proof. By (3.1.1)

$$Q_{p^r}(x) = \prod_{d|p^r} (x^{p^r/d} - 1)^{\mu(d)}$$

$$= (x^{p^r}-1)^{\mu(1)}(x^{p^{r-1}}-1)^{\mu(p)}(x^{p^{r-2}}-1)^{\mu(p^2)} \cdots (x^{p}-1)^{\mu(p^{r-1})}(x-1)^{\mu(p^r)}$$

$$= (x^{p^r}-1)(x^{p^{r-1}}-1)^{-1}$$

$$= \frac{(x^{p^r}-1)}{(x^{p^{r-1}}-1)}$$

On the other hand

$$Q_p(x^{p^{r-1}}) = \prod_{d|p} ((x^{p^{r-1}})^{p/d}-1)^{\mu(d)}$$

$$= ((x^{p^{r-1}})^{p}-1)^{\mu(1)} \cdot ((x^{p^{r-1}})-1)^{\mu(p)}$$

$$= ((x^{p^{r-1}})^{p}-1)((x^{p^{r-1}})-1)^{-1}$$

$$= \frac{(x^{p^r}-1)}{(x^{p^{r-1}}-1)}$$

Thus $Q_{p^r}(x) = Q_p(x^{p^{r-1}})$. ∎

Identity 3.3. For $n = p_1^{r_1} \cdots p_s^{r_s}$

$$Q_n(x) = Q_{p_1 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$$

Proof. By (3.1.1)

$$Q_{p_1^{r_1} \cdots p_s^{r_s}}(x) = \frac{(x^n - 1)\,\Pi(x^{n/p_i p_j} - 1) \cdots}{\Pi(x^{n/p_i} - 1)\,\Pi(x^{n/p_i p_j p_k} - 1) \cdots}$$

where $i, j, \cdots$ range from $1, \cdots, s$ and in the denominator the products extend over the combinations $1, 3, 5, \cdots$ at a time of $p_1, p_2, \cdots, p_s$; in the numerator, $2, 4, 6, \cdots$ at a time.

On the other hand

$$Q_{p_1 p_2 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}}) = \frac{((x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})^m - 1)\,\Pi((x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})^{m/p_i p_j} - 1) \cdots}{\Pi((x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})^{m/p_i} - 1)\,\Pi((x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})^{m/p_i p_j p_k} - 1) \cdots}$$

$$= \frac{(x^n - 1)\,\Pi(x^{n/p_i p_j} - 1) \cdots}{\Pi(x^{n/p_i} - 1)\,\Pi(x^{n/p_i p_j p_k} - 1) \cdots}$$

where $m = p_1 p_2 \cdots p_s$.

Thus $Q_{p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}}(x) = Q_{p_1 p_2 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$ ∎

Identity 3.4. If n is odd, then

$$Q_{2n}(x) = Q_n(-x) .$$

Proof. Let $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ where n is odd. Then by (3.1.1)

$$Q_{2n}(x) = \frac{(x^{2n}-1)(\Pi(x^{2n/2p_i}-1)\,\Pi(x^{2n/p_ip_j}-1)\cdots}{((x^{2n/2}-1)\Pi(x^{2n/p_i}-1))(\Pi(x^{2n/2p_ip_j}-1)\Pi(x^{2n/p_ip_jp_k}-1))\cdots}$$

$$= \frac{(x^{n}-1)(x^{n}+1)(\Pi(x^{n/p_i}-1)\Pi(x^{2n/p_ip_j}-1)\cdots}{((x^{n}-1)\Pi(x^{2n/p_i}-1))(\Pi(x^{n/p_ip_j}-1)\Pi(x^{2n/p_ip_jp_k}-1)\cdots}$$

$$= \frac{(x^{n}+1)(\Pi(x^{n/p_i}-1)\,\Pi(x^{2n/p_ip_j}-1))\cdots}{\Pi(x^{2n/p_i}-1)(\Pi(x^{n/p_ip_j}-1)\,\Pi(x^{2n/p_ip_jp_k}-1)\cdots}$$

$$= \frac{(x^{n}+1)\Pi(x^{n/p_i}-1)\,\Pi((x^{n/p_ip_j}-1)(x^{n/p_ip_j}+1))\cdots}{\Pi((x^{n/p_i}-1)(x^{n/p_i}+1))\,\Pi(x^{n/p_ip_j}-1)\,\Pi((x^{n/p_ip_jp_k}-1)(x^{n/p_ip_jp_k}+1))\cdots}$$

$$= \frac{(x^{n}+1)\,\Pi(x^{n/p_ip_j}+1)\,\Pi(x^{n/p_ip_jp_kp_t}+1)\cdots}{\Pi(x^{n/p_i}+1)\,\Pi(x^{n/p_ip_jp_k}+1)\,\Pi(x^{n/p_ip_jp_kp_tp_u}+1)\cdots}$$

On the other hand

$$Q_n(-x) = \frac{((-x)^n - 1)\Pi((-x)^{n/p_ip_j} - 1)\cdots}{\Pi((-x)^{n/p_i} - 1)\Pi((-x)^{n/p_ip_jp_k} - 1)\cdots}$$

$$= \frac{-(x^n+1)\,\Pi((-x)^{n/p_ip_j} - 1)\cdots}{\Pi((-x)^{n/p_i} - 1)\Pi((-x)^{n/p_ip_jp_k} - 1))\cdots}$$

$$= \frac{(-1)(x^n+1)(-1)^{s}C_2\,\Pi(x^{n/p_ip_j}+1)(-1)^{s}C_4\,\Pi(x^{n/p_ip_jp_kp_t}+1)\cdots}{(-1)^{s}C_1\,\Pi(x^{n/p_i}+1)(-1)^{s}C_3\,\Pi(x^{n/p_ip_jp_k}+1)(-1)^{s}C_5\,\Pi(x^{n/p_ip_jp_kp_tp_u}+1)\cdots}$$

$$= \frac{(-1)(-1)^{s}C_1(-1)^{s}C_2\cdots(-1)^{s}C_s(x^n+1)\,\Pi(x^{n/p_ip_j}+1)\,\Pi(x^{n/p_ip_jp_kp_t}+1)\cdots}{\Pi(x^{n/p_i}+1)\,\Pi(x^{n/p_ip_jp_k}+1)\,\Pi(x^{n/p_ip_jp_kp_tp_u}+1)\cdots}$$

but $(-1)^{s}C_1(-1)^{s}C_2\cdots(-1)^{s}C_s = (-1)^{{}_sC_1+{}_sC_2+\cdots+{}_sC_s}$ and

${}_sC_1 + {}_sC_2 + \cdots + {}_sC_3 = 2^s - 1$ so that $(-1)^{2^s-1} = -1$. Therefore

$$Q_n(-x) = \frac{(x^n+1)\,\Pi(x^{n/p_ip_j}+1)\,\Pi(x^{n/p_ip_jp_kp_t}+1)\cdots}{\Pi(x^{n/p_i}+1)\,\Pi(x^{n/p_ip_jp_k}+1)\,\Pi(x^{n/p_ip_jp_kp_tp_u}+1)\cdots}$$

Thus $Q_n(x) = Q_n(-x)$ ∎

Identity 3.5. If p is a prime, not dividing n,

$$Q_{pn}(x) = \frac{Q_n(x^p)}{Q_n(x)}$$

Proof. Let $n = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ where $p \nmid n$ then by (3.1.1)

$$Q_{pn}(x) = \frac{(x^{pn}-1)(\Pi(x^{pn/p_i}-1)(\Pi(x^{pn/p_ip_j}-1)\Pi(x^{pn/p_ip_jp_k}-1)\Pi(x^{pn/p_ip_jp_kp_t}-1)\cdots}{((x^{pn/p_i}-1)\Pi(x^{pn/p_ip_j}-1))(\Pi(x^{pn/p_ip_jp_k}-1)\cdots}$$

$$= \frac{(x^{pn}-1)\Pi(x^{n/p_i}-1)\Pi(x^{pn/p_ip_j}-1)\Pi(x^{n/p_ip_jp_k}-1)\cdots}{(x^{n}-1)\Pi(x^{pn/p_i}-1)\Pi(x^{n/p_ip_j}-1)\Pi(x^{pn/p_ip_jp_k}-1)\cdots}$$

On the other hand

$$\frac{Q_n(x^p)}{Q_n(x)} = \frac{\dfrac{((x^p)^n-1)\Pi((x^p)^{n/p_ip_j}-1)\cdots}{\Pi((x^p)^{n/p_i}-1)\Pi((x^p)^{n/p_ip_jp_k}-1)\cdots}}{\dfrac{(x^n-1)\Pi(x^{n/p_ip_j}-1)\cdots}{\Pi(x^{n/p_i}-1)\Pi(x^{n/p_ip_jp_k}-1)\cdots}}$$

$$= \frac{(x^{pn}-1)\Pi(x^{n/p_i}-1)\Pi(x^{pn/p_ip_j}-1)\Pi(x^{n/p_ip_jp_k}-1)\cdots}{(x^{n}-1)\Pi(x^{pn/p_i}-1)\Pi(x^{n/p_ip_j}-1)\Pi(x^{pn/p_ip_jp_k}-1)\cdots}$$

Thus $$Q_{pn}(x) = \frac{Q_n(x^p)}{Q_n(x)}$$ ∎

§2. On the Coefficients in Case of $n = pq$

By definition of the cyclotomic polynomial $Q_n(x)$, for $n = pq$ ($p < q$, primes), is given by

$$(3.2.1) \qquad Q_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x^{p}-1)(x^{q}-1)}$$

A. Migotti in 1883 and A. S. Bang in 1895 have proved that the coefficients of $Q_{pq}(x)$ are ± 1 or 0. In a recent paper Sister Marion Beiter in 1964 has given another proof of it. She also has determined the middle coefficient of $Q_{pq}(x)$. In 1966 L. Carlitz has determined the number of non-zero terms in $Q_{pq}(x)$.

In this section we shall review these theorems one by one.

Theorem 3.6. (General Coefficients)

Let $Q_{pq}(x) = \sum_{m=0}^{\phi(pq)} c_m x^m$. In $Q_{pq}(x)$

$$(3.2.2) \qquad c_m = \begin{cases} (-1)^{\delta} & \text{if } m = \alpha q + \beta p + \delta \text{ in exactly one way,} \\ 0 & \text{otherwise} \end{cases}$$

where $\phi(pq)$ is Euler's ϕ-function and α, β are nonnegative integers and $\delta = 0, 1$.

Proof. From (3.2.1) it follows that

$$Q_{pq}(x) = (x^{pq}-1)(x-1)/(x^{p}-1)(x^{q}-1)$$

$$= (1-x)(1+x^{q}+\cdots+)(^{(p-1)q})(1+x^{p}+x^{2p}+\cdots)$$

$$= \sum_{\alpha=0}^{p-1} x^{\alpha q} \sum_{\beta=0}^{\infty} x^{\beta p} - \sum_{\alpha=0}^{p-1} x^{\alpha q+1} \sum_{\beta=0}^{\infty} x^{\beta p}$$

$$= \sum_{\alpha,\beta,\delta} (-1)^{\delta} x^{\alpha q+\beta p+\delta},$$

where α runs through the integers from zero to $p-1$, β is any nonnegative integer, and $\delta=0,1$. Then c_m in $Q_{pq}(x)$ is the sum of the coefficients of all terms on the right with exponent $\alpha q+\beta p+\delta=m$. Where no such partition exists, c_m is zero. If there is exactly one partition, c_m equals $(-1)^{\delta}$.

Assume that m can be partitioned in two ways,

$$m = \alpha_1 q + \beta_1 p + \delta_1$$

$$= \alpha_2 q + \beta_2 p + \delta_2$$

with $\delta_1=\delta_2$. Then $q(\alpha_1-\alpha_2)=p(\beta_2-\beta_1)$. This implies that p divides $\alpha_1-\alpha_2$. But since $\alpha < p$, $|\alpha_1-\alpha_2| < p$. Therefore $\alpha_1-\alpha_2=\beta_2-\beta_1=0$, and the two partitions are identical. Hence, when two distinct partitions of m in the form (3. 2. 2) exist, in one of them $\delta = 1$, in the other $\delta = 0$. In this case c_m is

$(-1)^1+(-1)^0 = 0$, and the theorem is proved. ∎

Theorem 3.7. (Midterm Coefficient)

In $Q_{pq}(x)$, when $m=\phi(pq)/2$, $c_m=(-1)^{k-1}$, where k is the least positive solution of the congruence $px \equiv 1 \pmod q$.

Proof. Set $m = \phi(pq)/2$ in (3.2.2). Then

$$(p-1)(q-1)/2 = \alpha q + \beta p + \delta$$

$$p(2\beta + 1) \equiv 1 - 2\delta \pmod q,$$

$$px \equiv \pm \pmod q \quad \text{where} \quad x = 2\beta + 1$$

Let k be the solution of $px \equiv 1 \pmod q$, $1 \leq k \leq q-1$. Then $q-k$ is a solution of $px \equiv -1 \pmod q$.

Consider $pk \equiv 1 \pmod q$. Then

$$pk = 1 + qh \qquad h = (pk - 1)/q,$$

$$\beta = (k - 1)/2 \qquad \alpha = (p - 1)/2 - h/2.$$

In the case k is odd, these values of α and β are integral, $\delta = 0$, and the midterm coefficient is 1.

If k is even, $q-k$ is odd, $\delta=1$, and the midterm coefficient is -1. Thus the theorem is proved. ∎

Remarks. In the special case $q = sp+1$, k is odd and the midterm coefficient is $+1$. Similarly, for $q = sp-1$, k is even and the midterm coefficient is -1.

In any case, the roles of p and q in the congruences may be reversed, without affecting the oddness or evenness of k.

The following table gives the value of the midterm coefficient c_m of $Q_{pq}(x)$ when p is 3, 5, or 7. All values of $n=pq$ and less than 143 reduce to one of these special cases.

p	a	c_m
3		
5	1, 2	± 1
7	1, 3, 5	

according as $q \equiv \pm a \pmod{p}$.

Theorem 3.8. (The Number of Nonzero Terms)

Let $\theta_0(pq)$ denote the number of terms with positive coefficients in $Q_{pq}(x)$. Take $q > p$ and define u by means of $qu \equiv -1 \pmod{p}$ $(0 < u < p)$. Then we have

$$\theta_o(pq) = (p-u)(uq+1)/p.$$

Proof. Let $\theta_0(pq)$ denote the number of terms with positive coefficients, $\theta_1(pq)$ the number of terms with negative coefficients and $\theta(pq) = \theta_0(pq) + \theta_1(pq)$, the total number of nonzero terms.

Since $Q_{pq}(1) = 1$ it follows at once that $\theta_0(pq)=1+\theta_1(pq)$, so that

$$\theta(pq) = 2\theta_0(pq)-1. \tag{3.2.3}$$

We may assume $q > p$ and define u by means of

(3.2.4) $\qquad qu \equiv -1 \pmod{p} \qquad (0 < u < p)$

Then by (3.2.1) we have

$$Q_{pq}(x) = \frac{1-x}{1-x^p} \sum_{j=0}^{p-1} x^{jq} = \frac{1}{1-x^p} \left\{ \sum_{j=0}^{p-1} x^{jq} - \sum_{i=0}^{p-1} x^{iq+1} \right\}$$

with each term x^{jq} of the first sum on the extreme right, associate the term x^{iq+1} of the second sum for which $iq+1 \equiv jq \pmod{p}$.

By (3.2.4) it follows that $i \equiv j+u \pmod{p}$. Then

$$(3.2.5)\quad Q_{pq}(x) = \frac{1}{1-x^p} \sum_{\substack{j=0 \\ j+u<p}}^{p-1} (x^{jq} - x^{(j+u)q+1}) + \frac{1}{1-x^p} \sum_{\substack{j=0 \\ j+u\geq p}}^{p-1} (x^{jq} - x^{(j+u-p)q+1})$$

$$= \frac{1-x^{uq+1}}{1-x^p} \sum_{j=0}^{p-1-u} x^{jq} - \frac{1-x^{(p-u)q-1}}{1-x^p} \sum_{i=0}^{u-1} x^{iq+1}$$

The first sum in (3.2.5) consists of the terms of $Q_{pq}(x)$ with positive coefficients; there are evidently $(p-u)(uq+1)/p$ such terms. The second sum in (3.2.5) accounts for the negative terms of $Q_{pq}(x)$; there are $u(pq-uq-1)/p$

$$\frac{(p-u)(uq+1)}{p} - \frac{u(pq-uq-1)}{p} = 1,$$

as we should expect.

This proves the theorem. ∎

Examples and Remarks

1. If $p = 3$ and $q = 3k+1$ and $3k+2$, then $u = 2$ and $u = 1$, respectively, so that

$$\theta_0(3(3k+1)) = 2k+1$$

$$\theta_0(3(3k+2)) = 2k+2$$

2. If $p = 5$ and $q = 5k+1$, $5k+2$, $5k+3$ and $5k+4$, then $u = 4, 2, 3$ and 1 respectively, so that

$$\theta_0(5(5k+1)) = 4k+1$$

$$\theta_0(5(5k+2)) = 6k+3$$

$$\theta_0(5(5k+3)) = 6k+4$$

$$\theta_0(5(5k+4)) = 4k+4$$

We remark that if we assume only that p and q are relatively prime but otherwise arbitrary integers greater than one, the above theorem continues to hold.

The notation is somewhat ambiguous; to avoid confusion we may write $Q_{p,q}(x)$ in place of $Q_{pq}(x)$ and $\theta_0(p, q)$ in place of $\theta_0(pq)$. Then we have, for example

$$\theta_0(4, 4k+1) = 3k+1,$$

$$\theta_0(4, 4k+3) = 3k+3.$$

3. Also for arbitrary p we have

$$\theta_0(p, kp+1) = k(p-1) + 1$$

$$\theta_0(p, kp+p-1) = k(p-1) + p - 1$$

For p odd, on the other hand, we get

$$\theta_0(p,\ kp+2) = \frac{1}{4}k(p^2-1) + \frac{1}{2}(p+1),$$

$$\theta_0(p, kp+p-2) = \frac{1}{4}(k+1)p^2-1) - \frac{1}{2}(p-1)$$

The last four formulas indicate how strongly the value of $\theta_0(p, q)$ depends on the residue of $q(\text{mod } p)$.

§3. The Coefficients of $Q_n(x)$ for $n < 105$

One of the most striking properties of the cyclotomic polynomial $Q_n(x)$ is the smallness of its coefficients.

We have seen in §2 of this chapter that the coefficients of the cyclotomic polynomial $Q_n(x)$ for $n=pq$, where p, q are distinct primes, are all ± 1 or 0.

Also we have verified a few identities about the cyclotomic polynomial in §1 of this chapter.

Using these identities and the theorems we can easily verify that in fact the coefficients of all cyclotomic polynomials $Q_n(x)$ for $n < 105$ are ± 1 or 0.

From definition of the cyclotomic polynomial we have $Q_1(x) = x-1$. Now we shall quote the theorem and identities in §1 and §2 and demonstrate this fact in Table I.

Table I. On the coefficients of $Q_n(x)$ for $n < 105$.

$Q_n(x)$	Factorization of n	Theorem and Identities Applied	Concerned $Q_n(x)$	$Q_n(x)$	Factorization of n	Theorem and Identities Applied	Concerned $Q_n(x)$	$Q_n(x)$	Factorization of n	Theorem and Identities Applied	Concerned $Q_n(x)$
Q_1	$n = 1$	Def.		Q_{20}	$n = 2^2 \cdot 5$	(3)	Q_{10}	Q_{39}	$n = 3 \cdot 13$	(6)	
Q_2	Prime	(1)		Q_{21}	$n = 3 \cdot 7$	(6)		Q_{40}	$n = 2^3 \cdot 5$	(3)	Q_{10}
Q_3	Prime	(1)		Q_{22}	$n = 2 \cdot 11$	(6)		Q_{41}	Prime	(1)	
Q_4	$n = 2^2$	(2)	Q_2	Q_{23}	Prime	(1)		Q_{42}	$n = 2 \cdot 3 \cdot 7$	(4)	Q_{21}
Q_5	Prime	(1)		Q_{24}	$n = 2^3 \cdot 3$	(3)	Q_6	Q_{43}	Prime	(1)	
Q_6	$n = 2 \cdot 3$	(6)		Q_{25}	$n = 5^2$	(2)	Q_5	Q_{44}	$n = 2^2 \cdot 11$	(3)	Q_{22}
Q_7	Prime	(1)		Q_{26}	$n = 2 \cdot 13$	(6)		Q_{45}	$n = 3^2 \cdot 5$	(3)	Q_{15}
Q_8	$n = 2^3$	(2)	Q_2	Q_{27}	$n = 3^3$	(2)	Q_3	Q_{46}	$n = 2 \cdot 23$	(4)	Q_{23}
Q_9	$n = 3^2$	(2)	Q_3	Q_{28}	$n = 2^2 \cdot 7$	(3)	Q_{14}	Q_{47}	Prime	(1)	
Q_{10}	$n = 2 \cdot 5$	(6)		Q_{29}	Prime	(1)		Q_{48}	$n = 2^4 \cdot 3$	(3)	Q_6
Q_{11}	Prime	(1)		Q_{30}	$n = 2 \cdot 3 \cdot 5$	(4)	Q_{15}	Q_{49}	$n = 7^2$	(2)	Q_7
Q_{12}	$n = 2^2 \cdot 3$	(3)	Q_6	Q_{31}	Prime	(1)		Q_{50}	$n = 2 \cdot 5^2$	(3)	Q_{10}
Q_{13}	Prime	(1)		Q_{32}	$n = 2^5$	(2)	Q_2	Q_{51}	$n = 3 \cdot 17$	(6)	
Q_{14}	$n = 2 \cdot 7$	(6)		Q_{33}	$n = 3 \cdot 11$	(6)		Q_{52}	$n = 2^2 \cdot 13$	(3)	Q_{26}
Q_{15}	$n = 3 \cdot 5$	(6)		Q_{34}	$n = 2 \cdot 17$	(6)		Q_{53}	Prime	(1)	
Q_{16}	$n = 2^4$	(2)	Q_2	Q_{35}	$n = 5 \cdot 7$	(6)		Q_{54}	$n = 2 \cdot 3^3$	(3)	Q_6
Q_{17}	Prime	(1)		Q_{36}	$n = 2^2 \cdot 3^2$	(3)	Q_6	Q_{55}	$n = 5 \cdot 11$	(6)	
Q_{18}	$n = 2 \cdot 3^2$	(3)	Q_6	Q_{37}	Prime	(1)		Q_{56}	$n = 2^3 \cdot 7$	(3)	Q_{14}
Q_{19}	Prime	(1)		Q_{38}	$n = 2 \cdot 19$	(6)		Q_{57}	$n = 3 \cdot 19$	(6)	

Table I (continued)

$Q_n(x)$	Factorization of n	Theorem and Identities Applied	Concerned $Q_n(x)$	$Q_n(x)$	Factorization of n	Theorem and Identities Applied	Concerned $Q_n(x)$	$Q_n(x)$	Factorization of n	Theorem and Identities Applied	Concerned $Q_n(x)$
Q_{58}	$n = 2 \cdot 29$	(6)		Q_{77}	$n = 7 \cdot 11$	(6)		Q_{96}	$n = 2^5 \cdot 3$	(3)	Q_6
Q_{59}	Prime	(1)		Q_{78}	$n = 2 \cdot 3 \cdot 13$	(4)	Q_{39}	Q_{97}	Prime	(1)	
Q_{60}	$n = 2^2 \cdot 3 \cdot 5$	(3)	Q_{30}	Q_{79}	Prime	(1)		Q_{98}	$n = 2 \cdot 7^2$	(3)	Q_{14}
Q_{61}	Prime	(1)		Q_{80}	$n = 2^4 \cdot 5$	(3)	Q_{10}	Q_{99}	$n = 3^2 \cdot 11$	(3)	Q_{33}
Q_{62}	$n = 2 \cdot 31$	(6)		Q_{81}	$n = 3^4$	(2)	Q_3	Q_{100}	$n = 2^2 \cdot 5^2$	(3)	Q_{10}
Q_{63}	$n = 3^2 \cdot 7$	(3)	Q_{21}	Q_{82}	$n = 2 \cdot 41$	(6)		Q_{101}	Prime	(1)	
Q_{64}	$n = 2^6$	(2)	Q_2	Q_{83}	Prime	(1)		Q_{102}	$n = 2 \cdot 3 \cdot 17$	(4)	Q_{51}
Q_{65}	$n = 5 \cdot 13$	(6)		Q_{84}	$n = 2^2 \cdot 3 \cdot 7$	(3)	Q_{42}	Q_{103}	Prime	(1)	
Q_{66}	$n = 2 \cdot 3 \cdot 11$	(4)	Q_{33}	Q_{85}	$n = 5 \cdot 17$	(6)		Q_{104}	$n = 2^2 \cdot 13$	(3)	Q_{26}
Q_{67}	Prime	(1)		Q_{86}	$n = 2 \cdot 43$	(6)					
Q_{68}	$n = 2^2 \cdot 17$	(3)	Q_{34}	Q_{87}	$n = 3 \cdot 29$	(6)					
Q_{69}	$n = 3 \cdot 23$	(6)		Q_{88}	$n = 2^3 \cdot 11$	(3)	Q_{22}				
Q_{70}	$n = 2 \cdot 5 \cdot 7$	(4)	Q_{35}	Q_{89}	Prime	(1)					
Q_{71}	Prime	(1)		Q_{90}	$n = 2 \cdot 5 \cdot 9$	(4)	Q_{45}				
Q_{72}	$n = 2^3 \cdot 3^2$	(3)	Q_6	Q_{91}	$n = 7 \cdot 13$	(6)					
Q_{73}	Prime	(1)		Q_{92}	$n = 2^2 \cdot 23$	(3)	Q_{46}				
Q_{74}	$n = 2 \cdot 37$	(6)		Q_{93}	$n = 3 \cdot 31$	(6)					
Q_{75}	$n = 3 \cdot 5^2$	(3)	Q_{15}	Q_{94}	$n = 2 \cdot 47$	(6)					
Q_{76}	$n = 2^2 \cdot 19$	(3)	Q_{38}	Q_{95}	$n = 5 \cdot 19$	(6)					

(1) If p is a prime, $Q_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$

(2) If p is a prime, and for an integer $r \geq 1$

$$Q_{p^r}(x) = Q_p(x^{p^{r-1}})$$

(3) For $n = p_1^{r_1} \cdots p_s^{r_s}$, $Q_{p_1^{r_1} \cdots p_s^{r_s}}(x) = Q_{p_1 \cdots p_s}(x^{p_1^{r_1-1} \cdots p_s^{r_s-1}})$

(4) If n is odd, then $Q_{2n}(x) = Q_n(-x)$

(5) If p is a prime, not dividing n,

$$Q_{pn}(x) = \frac{Q_n(x^p)}{Q_n(x)}$$

(6) For $n = pq$, the coefficients of $Q_{pq}(x)$ are ± 1 or 0.

CHAPTER 4. THE ANALYSIS AND CORRECTIONS TO E. LEHMER'S PAPER

§1. Schur's and Bungers' Theorem

In this section, before going to discuss E. Lehmer's paper we shall state Schur's theorem and Bungers' theorem.

Theorem 4.1. (Schur's Theorem)

There exist cyclotomic polynomials with coefficients arbitrarily large in absolute value.

Proof.[7] (12). Let $n = p_1 p_2 \cdots p_t$, where t is odd and $p_1 < p_2 < \cdots < p_t$ are odd primes such that $p_1 + p_2 > p_t$. To prove the theorem it is sufficient to show that the coefficient of x^{p_t} in $Q_n(x)$ is $1-t$. This can be done by taking $Q_n(x)$ modulo x^{p_t+1} we then get

$$\begin{aligned} Q_n(x) &\equiv \prod_{i=1}^{t}(1-x^{p_i})/(1-x) \\ &\equiv (1+x+\cdots+x^{p_t-1})(1-x^{p_1})(1-x^{p_2})\cdots(1-x^{p_t-1}) \\ &\equiv (1+x+\cdots+x^{p_t-1})(1-x^{p_1}-x^{p_2}-\cdots-x^{p_t-1}) \pmod{x^{p_t+1}} \end{aligned}$$

Collecting the coefficients of x^{p_t} in this last expression we see that it is precisely $-(t-1)$ so that as t increases we can exhibit

[7] This proof is credited to Schur.

arbitrarily large negative coefficients of the cyclotomic polynomials which proves the theorem. ∎

The question now remains as to the boundedness of the coefficients of $Q_n(x)$ for a fixed t. We have already seen that for $t=1$ and 2 these coefficients are actually 1, -1 or 0. The case $t=3$ was discussed by Bungers' who proved the following theorem.

Theorem 4.2. (Bungers' Theorem)[8]

As n runs over all products of three distinct primes, the cyclotomic polynomials $Q_n(x)$ contain arbitrarily large coefficients, provided there exist infinitely many prime pairs.

His proof depends on choosing three primes, two of which differ by 2, and in exhibiting a coefficient of $Q_{pqr}(x)$ equal to $(p+1)/2$.

§2. Corrections to E. Lehmer's Paper

E. Lehmer in 1936 modified Bungers' proof using Dirichlet's Theorem so as to eliminate the unproved assumption of the existence of infinitely many prime pairs, but she made a careless mistake in the process of proof. We shall now analyze her proof in detail and

---

[8] Göttingen Dissertation, 1934. The author has not seen the paper, which is quoted by Lehmer (12).

point out the part of the mistake and give a complete correct proof.

Let $n=pqr$, where $q=kp+2$, and $r=(mpq-1)/2$. For a given p such primes q and r can always be found by Dirichlet's Theorem.[9/]

We proceed to show that the coefficient of x^h, where $h = (p-3)(qr+1)/2$ is $(p-1)/2$ and hence can be made arbitrarily large with p.

From definition of the cyclotomic polynomial with $n = pqr$, we have

$$(4.2.1)\quad Q_{pqr}(x) = \prod_{d|pqr} (x^{pqr/d}-1)^{\mu(d)}$$

$$= (x^{pqr}-1)(x^{qr}-1)^{-1}(x^{pr}-1)^{-1}(x^{pq}-1)^{-1}(x^{r}-1)(x^{q}-1)(x^{p}-1)(x-1)^{-1}$$

$$= \frac{(x^{pqr}-1)(x^{p}-1)x^{q}-1)(x^{r}-1)}{(x-1)(x^{pq}-1)(x^{pr}-1)(x^{qr}-1)}$$

$$= (1+x+x^2+\cdots+x^{p-1})(1-x^{q}-x^{r}+x^{q+r}) \cdot \frac{(1-x^{pqr})}{(1-x^{pq})(1-x^{pr})(1-x^{qr})}$$

But

[9/] Dirichlet's Theorem: If a is positive and a and b are relatively primes, then there exist infinitely many primes of the form $an+b$.

$$\frac{(1-x^{pqr})}{(1-x^{pq})(1-x^{pr})(1-x^{qr})} = (1-x^{pqr})(1+x^{pq}+x^{2pq}+x^{3pq}+\cdots)(1+x^{qr}+x^{2qr}+x^{3qr}+\cdots)$$

$$\cdot (1+x^{pr}+x^{2pr}+x^{3pr}+\cdots)$$

$$= (1+x^{pq}+x^{2pq}+x^{3pq}+\cdots)(1+x^{qr}+x^{2qr}+x^{3qr}+\cdots)$$

$$\cdot (1+x^{pr}+x^{2pr}+x^{3pr}+\cdots) - x^{pqr}(1+x^{pq}+x^{2pq}+\cdots)$$

$$\cdot (1+x^{qr}+x^{2qr}+\cdots)(1+x^{pr}+x^{2pr}+\cdots)$$

$$\equiv (1+x^{pq}+x^{2pq}+\cdots)(1+x^{qr}+x^{2qr}+\cdots)(1+x^{pr}+x^{2pr}+\cdots) \pmod{x^{pqr}}$$

$$= \Sigma x^{\nu pq} \cdot \Sigma x^{\lambda qr} \cdot \Sigma x^{\mu pr}$$

$$= \Sigma x^{\nu pq+\lambda qr+\mu pr}$$

(4.2.1)' i.e. $$Q_{pqr}(x) \equiv (1+x+x^2+\cdots+x^{p-1})(1-x^q-x^r+x^{q+r}) \cdot \Sigma x^{\nu pq+\lambda qr+\mu pr} \pmod{x^{pqr}}$$

Since we are interested in the coefficient of x^h, the summation indices ν, λ, μ satisfy the following inequalities:

(4.2.2) $$\nu qr \leq h, \qquad \lambda pr \leq h, \qquad \mu pq \leq h.$$

We now consider the diophantine equation

(4.2.3) $$\nu qr + \lambda pr + \mu pq + \omega + \epsilon q + \eta r = (p-3)(qr+1)/2 = h$$

where $\omega < p$, and $\epsilon = 0$ or 1, $\eta = 0$ or 1.

The coefficient of x^h is now given by the number of solutions

of (4. 2. 3) with $\epsilon = \eta$ minus the number of solutions of (4. 2. 3) with $\epsilon \neq \eta$.

In the second parenthesis of the right side of (4. 2. 1)' if $\epsilon = \eta$ the signs of x are + and if $\epsilon \neq \eta$ the signs of x are -.

Taking (4. 2. 3) modulo $p, q,$ and r we have, since

$$qr = (kp+2) \cdot (mpq-1)/2 \equiv -1 \pmod{p}$$

$$\nu qr + \omega + \epsilon q + \eta r \equiv 0 \pmod{p},$$

$$\lambda pr + \omega + \eta r \equiv (p-3)/2 \pmod{q},$$

$$\mu pq + \omega + \epsilon q \equiv (p-3)/2 \pmod{r}.$$

Multiplying the last two congruences by k and m respectively, we then get

$$k\lambda pr + k\omega + k\eta r \equiv k(p-3)/2 \pmod{q}$$

$$k\mu pq + m\omega + m\epsilon q \equiv m(p-3)/2 \pmod{r}$$

but $kpr = kp(mpq-1)/2 = (q-2)(mpq-1)/2 \equiv 1 \pmod{q}$

$mpq = 2r + 1 \equiv 1 \pmod{r}$

and also $q \equiv 2 \pmod{p}$, $r \equiv -1/2 \pmod{pq}$.

Thus we get

(4. 2. 4) $\omega \equiv \nu - 2\epsilon + \eta/2 \pmod{p}$

(4. 2. 5) $\lambda \equiv k((p-3)/2 - \omega + \eta/2) \pmod{q}$

(4. 2. 6) $\mu \equiv m((p-3)/2 - \omega + \epsilon q) \pmod{r}$

We shall now show that if $\epsilon = \eta = 0$. (4. 2. 3) has $(p-1)/2$

solutions, while in the other three cases (4. 2. 3) has no solutions.

(I) If $\epsilon = \eta = 0$ (4. 2. 4) implies $\omega \equiv \nu \pmod{p}$ but $\omega < p$ and $\nu < p$, (4. 2. 4) becomes $\omega = \nu$ for, from (4. 2. 2)

$$\nu qr \leq h \implies \nu qr \leq \frac{(p-3)}{2}(qr+1)$$

$$\implies \nu \leq \frac{(p-3)}{2}$$

Equations (4. 2. 5) and (4. 2. 6) become in this case

$$\lambda \equiv k((p-3)/2 - \nu) \pmod{q}$$

$$\mu \equiv m((p-3)/2 - \nu) \pmod{r}$$

but also from (4. 2. 2)

$$\lambda pr \leq h \implies \lambda pr \leq \frac{(p-3)}{2}(qr+1)$$

$$\implies \lambda \leq \frac{(p-3)}{2} < p < q$$

$$\implies \lambda < q \quad \text{and} \quad k(p-3)/2 < q \quad \text{since} \quad q = kp+2.$$

$$\mu pq \leq h \implies \mu pq \leq \frac{(p-3)}{2}(qr+1)$$

$$\implies \mu \leq \frac{(p-3)}{2} < r$$

$$\implies \mu < r \quad \text{and} \quad m(p-3)/2 < r \quad \text{since} \quad r = (mpq-1)/2.$$

Therefore these congruences are actually equalities, and since $\nu \leq (p-3)/2$, we can take 0 through $(p-3)/2$ as values of ν and we have determined for each of the $(p-1)/2$ values of ν, corresponding values of λ and μ, which are such that

$\lambda \leq k(p-3)/2$, so that

$$\lambda pr \leq kpr(p-3)/2 < qr(p-3)/2 < h ,$$

and $\mu \leq m(p-3)/2$ so that

$$\mu pq \leq mpq(p-3)/2 \overset{10/}{=} (2r+1)(p-3)/2 < h ,$$

so that all the variables are determined within the range (4.2.2) and hence in the case $\epsilon = \eta = 0$ (4.2.3) has $(p-1)/2$ solutions.

(II) For $\epsilon = 1$, $\eta = 0$ (4.2.4) gives us $\omega \equiv \nu - 2 \pmod p$, where $0 \leq \omega < p$ and $0 \leq \nu \leq (p-3)/2$. But $\omega < p$, and $\nu - 2 < p$. We then get $\omega = \nu - 2$.

Also $\omega \equiv \nu - 2 \pmod p$ implies $\omega = tp + \nu - 2$ for some integer t.

If $\nu = 0$ we have $\omega = tp - 2$ and $\omega < p$. Thus $t = 1$ and $\omega = p - 2$.

If $\nu = 1$ we have $\omega = tp - 1$ and $\omega < p$. Thus t also must be 1 and we get $\omega = p - 1$.

If $\nu \geq 2$ we have $\omega = tp + \ell - 2 \geq p$ for any integer $\ell \geq 2$ and $t \geq 1$, so that this contradicts the condition $\omega < p$.

Hence we have either $\omega = \nu - 2$, or $\omega = p - 1$, or $\omega = p - 2$.

In the last two cases we can use (4.2.5) to get

$\overset{10/}{}$In Lehmer's paper, $mpq(p-3)/2 \leq (2r+1)(p-3)/2$, and this is obviously a mistake since $r = (mpq-1)/2$.

$$\lambda = k((p-3)/2 - \omega) \equiv -k(p \pm 2)/2 \pmod{q}.$$

That is,

$$\lambda = q - k(p \pm 1)/2 \geq q - k(p-1)/2,$$

so that

$$\lambda pr \geq pqr - kpr(p-1)/2 > pqr - qr(p-1)/2 = qr(p+1)/2 > h,$$

for, $q = kp+2$ implies $q > kp$ and

$$qr(p+1)/2 - h = qr(p+1)/2 - (p-3)(qr+1)/2$$
$$= (4qr+3-p)/2 > 0.$$

Hence for $\omega = p-1$ or $\omega = p-2$, (4. 2. 2) is violated for λpr, and there are no solutions.

If $\omega = \nu - 2 \leq (p-7)/2$, we use (4. 2. 6) and obtain

$$\mu \equiv m((p-3)/2 - \omega - q) \pmod{r},$$

or

$$\mu = r + m((p-3)/2 - \omega - q) \geq r + m(2-q).$$

Hence

$$\mu pq \geq pqr + pqm(2-q)$$
$$= pqr + (2r+1)(2-q)$$
$$= (qr+1)(p-2) + (4r-p-q+4)$$
$$> (qr+1)(p-2) > h$$

so that (4. 2. 2) is again violated and there are no solutions of (4. 2. 3) for $\epsilon = 1$, $\eta = 0$.

(III) In the next case $\epsilon = 0$, $\eta = 1$, we get from (4.2.4)

$\omega \equiv \nu + \frac{1}{2} \pmod{p}$ [11] and $\nu \leq (p-3)/2$. But since $\omega < p$ $\nu + \frac{1}{2} < p$, we have $\omega = \nu + \frac{1}{2}$. Putting this value for ω in (4.2.6), we have

$$\mu \equiv m((p-3)/2 - \nu - \frac{1}{2}) \pmod{r},$$

or

$$\mu = r + m((p-4)/2 - \nu) \geq r - \frac{1}{2} m.$$

Hence

$$upq \geq pqr - \frac{1}{2} pqm$$

$$= pqr - \frac{1}{2}(2r+1)$$

$$= (qr+1)(p-2) + (2qr + \frac{3}{2} - r - p)$$

$$> (qr+1)(p-2) > h.$$

Thus this case also does not yield any further solutions.

(IV) In the last case $\epsilon = \eta = 1$ [12] we get from (4.2.4) $\omega \equiv \nu - \frac{3}{2}$ (mod p), but by the same reason as (III) we have $\omega = \nu - \frac{3}{2}$ and with the same procedure as above we get

$$\mu \equiv m((p-3)/2 - \nu + \frac{3}{2} - q) \pmod{r},$$

or

$$\mu = r + m(p/2 - \nu - q) \geq r + m(\frac{3}{2} - q).$$

---

[11] E. Lehmer made a careless mistake in this part. She got from (4.2.4) $\omega = \nu(p+1)/2$, but this is obviously wrong, so that her proof of this part must be corrected.

[12] In Lehmer's paper, the proof of this case is abbreviated.

Hence

$$\mu pq \geq pqr + pqm\left(\frac{3}{2} - q\right)$$

$$= pqr + (2r+1)\left(\frac{3}{2} - q\right)$$

$$= (qr+1)(p-2) + \left(3r + \frac{7}{2} - q - p\right)$$

$$> (qr+1)(p-2) > h .$$

Thus this case does not contribute any solutions.

Therefore the coefficient of x^h increases with p, so that we have proved the following theorem.

Theorem 4.3 (Lehmer's Theorem)

As n runs over all product of three distinct primes the cyclotomic polynomial $Q_n(x)$ contain arbitrarily large coefficients.

CHAPTER 5. A GENERAL FORMULA AND ITS APPLICATIONS

§1. Hölder's Formula and Newton's Identities

In 1936 O. Hölder gave a simple formula for the "Ramanujan sum" and in 1953 E. Gagliardo obtained it in another way. We shall condense the argument of Hölder in the following.

By a "Ramanujan sum" we mean most often the sum of the k^{th} powers of the primitive n^{th} roots of unity

$$C_n(k) = \sum_{(\ell,n)=1} e^{\frac{2\pi i \ell}{n} k} \tag{5.1.1}$$

Ramanujan has given the value of this sum as

$$C_n(k) = \sum_{d \mid (n,k)} \mu(\tfrac{n}{d})\, d \tag{5.1.2}$$

in which the dummy variable d ranges over all common divisors of n and k.

This value can be represented in a simpler form. We shall next deduce this, that (5.1.2) for $k = 1$, i.e., for the sum of the primitive n^{th} roots of unity

$$C_n(1) = \mu(n) \tag{5.1.3}$$

If we cancel the greatest common divisors of n and k in the terms of (5.1.1) there results

$$(5.1.4) \qquad C_n(k) = \sum_{(\ell, n)=1} e^{\frac{2\pi i \ell k'}{n'}}$$

in which

$$(5.1.5) \qquad n = \tau n'$$

$$k = \tau k'$$

$$\text{with} \qquad (n', k') = 1$$

Since ℓ runs through the numbers less than n and relatively prime to n and hence to n', $\ell k'$ is also relatively prime to n' and the sum (5.1.4) consists of $\phi(n)$ terms, all being primitive n'^{th} roots of unity but not all are distinct.

We can set, when ℓ' runs through the numbers $\leq n'$ and relatively prime to n',

$$(5.1.6) \qquad C_n(k) = \sum_{(\ell', n')\ 1} a_{\ell'} e^{\frac{2\pi i \ell'}{n'}}$$

$$= \sum_{(\ell', n')=1} a_{\ell'} (e^{\frac{2\pi i}{n'}})^{\ell'},$$

in which $a_{\ell'}$ are positive integers whose sum is equal to $\phi(n)$.

The polynomial $Q_n(x)$ is an irreducible factor of $x^n - 1$ with integer coefficients and leading coefficient 1.

The sum of the k^{th} powers of the roots of equation $Q_n(x) = 0$ is therefore an integer, positve, negative or equal to zero.

On account of the irreducibility of $Q_n(x) = 0$, we can put into (5.1.6) in place of the root $e^{\frac{2\pi i}{n'}}$ any other root $e^{\frac{2\pi i}{n'} h'}$ of the equation, h' being relatively prime to n'.

Thereby results the relation

$$C_n(k) = \sum_{(\ell', n')=1} a_{\ell'} e^{\frac{2\pi i}{n'} \ell' h'}$$

In this we now let h' range over the totality $\phi(n')$ of numbers $\leq n'$ and relatively prime to n' and sum once again. On the right appears each $a_{\ell'}$ multiplied by the sum of all $\phi(n')$ primitive n'^{th} roots of unity, which, by (5.1.3) is equal to $\mu(n')$ and we get

$$\phi(n') \cdot C_n(k) = \Big(\sum_{(\ell', n')=1} a_{\ell'} \Big) \mu(n')$$

by (5.1.1)

$$C_{n'}(h') = \sum_{(\ell', n')=1} e^{\frac{2\pi i \ell'}{n'} h'}$$

and if $h' = 1$, then by (5.1.3)

$$C_{n'}(1) = \sum e^{\frac{2\pi i \ell'}{n'}} = \mu(n')$$

However, since the sum of the $a_{\ell'}$ is equal to $\phi(n)$, we get

$$C_n(k) = \frac{\phi(n)}{\phi(n')}\ \mu(n')$$

that is, the Ramanujan sum

(5.1.7) $$C_n(k) = \frac{\phi(n)}{\phi(\frac{n}{\tau})}\ \mu(\frac{n}{\tau})$$

in which τ is the greatest common divisor of n and k.

Thus we call (5.1.7) Hölder's formula.

In order to use (5.1.7) we shall need Newton's identities on the sums of power of roots of equations. We give a discussion below which is based on the text of Oskar Perron (14, p. 150-151).

Let

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n.$$

The sums

(5.1.8) $$S_m = x_1^m + x_2^m + \cdots + x_n^m \qquad (m = 0, 1, 2, \cdots)$$

where x_i, $i = 1, 2, \cdots, n$ are roots of $f(x)$ are obviously

(5.1.9) $$S_0 = n, \quad S_1 = -a_1$$

We can write $f(x)$ as

(5.1.10) $$f(x) = (x-x_1)(x-x_2)\cdots(x-x_n)$$

$$= x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

Then the derived polynomial of $f(x)$ is

$$(5.1.11) \qquad f'(x) = nx^{n-1} + (n-1)a_1 x^{n-2} + \cdots + a_{n-1}$$

On the other hand

$$(5.1.12) \qquad \frac{f'(x)}{f(x)} = \sum_{i=1}^{n} \frac{1}{x-x_i}$$

It follows that, by (5.1.10) obviously $f(x_i) = 0$. Thus

$$f'(x) = \sum_{i=1}^{n} \frac{f(x)}{x-x_i} = \sum_{i=1}^{n} \frac{f(x) - f(x_i)}{x-x_i}$$

but

$$\frac{f(x)-f(x_i)}{x-x_i} = x^{n-1} + x_i x^{n-2} + \cdots + x_i^{n-1}$$

$$+ a_1(x^{n-2} + x_i x^{n-3} + \cdots + x_i^{n-2}) + \cdots + a_{n-1}$$

$$= x^{n-1} + (x_i + a_1)x^{n-2} + (x_i^2 + a_1 x_i + a_2)x^{n-3}$$

$$+ \cdots + (x_i^{n-1} + a_1 x_i^{n-2} + \cdots + a_{n-1}).$$

We sum this on i and get

$$(5.1.13) \quad f'(x) = \sum_{i=1}^{n} \frac{f(x)-f(x_i)}{x-x_i} = nx^{n-1} + (S_1 + na_1)x^{n-2} + (S_2 + a_1 S_1 + na_2)x^{n-3}$$

$$+ \cdots + (S_{n-1} + a_1 S_{n-2} + \cdots + a_{n-2} S_1 + na_{n-1})$$

Since the right sides of formulas (5.1.11) and (5.1.13) represent the same polynomial $f'(x)$, their coefficients must be identical, therefore, after rearranging the resulting equations, we have

$$
\begin{aligned}
& S_1 + a_1 = 0 \\
& S_2 + a_1 S_1 + 2a_2 = 0 \\
& \cdots\cdots\cdots \\
& \cdots\cdots\cdots \\
& S_{n-1} + a_1 S_{n-2} + \cdots + a_{n-2} S_1 + (n-1) a_{n-1} = 0
\end{aligned}
\tag{5.1.14}
$$

We call (5.1.14) Newton's identities.

§2. General Formula

As mentioned in Chapter 2 we can define the cyclotomic polynomial as

$$
\begin{aligned}
Q_n(x) &= (x - \xi_1)(x - \xi_2)\cdots(x - \xi_{\phi(n)}) \\
&= \prod_{i=1}^{\phi(n)} (x - \xi_i)
\end{aligned}
\tag{5.2.1}
$$

where $\phi(n)$ is Euler's-function and ξ_i's are the primitive n^{th} roots of unity.

Since the product of all primitive n^{th} roots of unity is 1 we can write (5.2.1) as

$$
Q_n(x) = x^{\phi(n)} + a_1 x^{\phi(n)-1} + \cdots + a_{\phi(n)-1} x + 1 \tag{5.2.2}
$$

Now we want to find the coefficient a_k of $x^{\phi(n)-k}$, where $k = 1, 2, \cdots, \phi(n)-1$.

Since all roots of the cyclotomic polynomial $Q_n(x)$ are primitive n^{th} roots of unity and the Ramanujan sum is the sum of the k^{th} powers of the primitive n^{th} roots of unity, we can apply Hölder's formula to Newton's identities and get the following recursive formula.

$$C(k) + a_1 C(k-1) + a_2 C(k-2) + \cdots + a_{k-1} C(1) + k a_k = 0$$

That is

$$(5.2.3) \qquad a_k = -\frac{C(k) + a_1 C(k-1) + a_2 C(k-2) + \cdots + a_{k-1} C(1)}{k}$$

where $C(k) = C_n(k)$ and $C_n(k) = \dfrac{\mu\left(\frac{n}{(n,k)}\right)\phi(n)}{\phi\left(\frac{n}{(n,k)}\right)}$

§3. Applications of General Formula

Now we would like to show, using Hölder's formula all coefficients of the cyclotomic polynomials $Q_n(x)$ for $n=105$, and $n = 595$.

We will see in $Q_{105}(x)$ for the first time the coefficients that are other than ± 1 or 0, and in $Q_{595}(x)$ the coefficient of x^h where $h = (p-3)(qr+1)/2$ coincides with that of E. Lehmer's theorem.

(I) Since $n = 105 = 3 \cdot 5 \cdot 7$ the Euler function

$$\phi(105) = 105 \cdot (1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7}) = 48$$

so that the degree of $Q_{105}(x)$ is 48.

$$Q_{105}(x) = x^{48}+a_1x^{47}+a_2x^{46}+\cdots+a_{47}x+1$$

At first we want to get all values of $C_{105}(k)$ in which k ranges over the integers from 1 through 47.

We can rewrite Hölder's formula as

$$C_n(k) = \frac{\phi(n)}{\phi(\frac{n}{(n,k)})}\ \mu\ (\frac{n}{(n,k)})$$

where (n,k) is greatest common divisor of n and k.

Since we can factorize $n = 105$ the product of three primes 3, 5, and 7, for all values of k we consider the following 7 classes:

(1) the multiples of 3; 3, 6, 12, 18, 24, 27, $\cdots$

(2) the multiples of 5; 5, 10, 20, 25, 40 .

(3) the multiples of 7; 7, 14, 28.

(4) the multiples of 15; 15, 30, 45.

(5) the multiples of 21; 21, 42.

(6) the multiples of 35; 35.

(7) others; 1, 2, 4, 8, 11, 13, 16, $\cdots$,

For the numbers that are multiples of two primes, we put

these numbers in the class of the product of these two primes. For example, 30 is a multiple of 3 and 5 and also a multiple of the product of 3 and 5, namely 15, we put 30 in the class of the multiples of 15.

For each of the above classes we want to find, using Hölder's formula, the sum of k^{th} powers of the primitive 105^{th} roots of unity.

(i) The numbers of the class (7) are all relatively prime to 105, that is $(105, k) = 1$ so that we have $C_{105}(k) = \mu(105)$ and since $105 = 3 \cdot 5 \cdot 7$, we get $\mu(105) = -1$, therefore

$$C_{105}(k) = -1$$

(ii) For the class (1) of the multiples of 3, we have $(105, k) = 3$ so that

$$C_{105}(k) = \frac{\mu(\frac{105}{(105,k)}) \cdot \phi(105)}{\phi(\frac{105}{(105,k)})} = \frac{\mu(35)\phi(105)}{\phi(35)} = \frac{1 \times 48}{24} = 2 .$$

(iii) For the class (2) of the multiples of 5, we have $(105, k) = 5$, so that

$$C_{105}(k) = \frac{\mu(\frac{105}{(105,k)}) \cdot \phi(105)}{\phi(\frac{105}{(105,k)})} = \frac{\mu(21) \cdot \phi(105)}{\phi(21)} = \frac{1 \times 48}{12} = 4 .$$

(iv) For the class (3) of the multiples of 7, we have $(105, k) = 7$, so that

$$C_{105}(k) = \frac{\mu(\frac{105}{(105,k)})\cdot\phi(105)}{\phi(\frac{105}{(105,k)})} = \frac{\mu(15)\cdot\phi(105)}{\phi(15)} = \frac{1\times 48}{8} = 6.$$

(v) For the class (4) of the multiples of 15, we have $(105,k) = 15$, so that

$$C_{105}(k) = \frac{\mu(\frac{105}{(105,k)})\cdot\phi(105)}{\phi(\frac{105}{(105,k)})} = \frac{\mu(7)\cdot\phi(105)}{\phi(7)} = \frac{-1\times 48}{6} = -8.$$

(vi) For the class (5) of the multiples of 21, we have

$$C_{105}(k) = \frac{\mu(\frac{105}{(105,k)})\cdot\phi(105)}{\phi(\frac{105}{(105,k)})} = \frac{\mu(5)\cdot\phi(105)}{\phi(5)} = \frac{-1\times 48}{4} = -12.$$

(vii) For the class (6) of the multiples of 35, we have

$$C_{105}(k) = \frac{\mu(\frac{105}{(105,k)})\cdot\phi(105)}{\phi(\frac{105}{(105,k)})} = \frac{\mu(3)\cdot\phi(105)}{\phi(3)} = \frac{-1\times 48}{2} = -24.$$

Now, we can apply these results in the general formula and get all coefficients one by one as in the following table.

Table II. All coefficients and Ramanujan sums of $Q_n(x)$ for $n = 105$.

$C_{105}(k)$		a_k		$C_{105}(k)$		a_k		$C_{105}(k)$		a_k	
C(1)	-1	a_1	1	C(17)	-1	a_{17}	1	C(33)	2	a_{33}	1
C(2)	-1	a_2	1	C(18)	2	a_{18}	0	C(34)	-1	a_{34}	1
C(3)	2	a_3	0	C(19)	-1	a_{19}	0	C(35)	-24	a_{35}	1
C(4)	-1	a_4	0	C(20)	4	a_{20}	-1	C(36)	2	a_{36}	1
C(5)	4	a_5	-1	C(21)	-12	a_{21}	0	C(37)	-1	a_{37}	0
C(6)	2	a_6	-1	C(22)	-1	a_{22}	-1	C(38)	-1	a_{38}	0
C(7)	6	a_7	-2	C(23)	-1	a_{23}	0	C(39)	2	a_{39}	-1
C(8)	-1	a_8	-1	C(24)	2	a_{24}	-1	C(40)	4	a_{40}	-1
C(9)	2	a_9	-1	C(25)	4	a_{25}	0	C(41)	-1	a_{41}	-2
C(10)	4	a_{10}	0	C(26)	-1	a_{26}	-1	C(42)	-12	a_{42}	-1
C(11)	-1	a_{11}	0	C(27)	2	a_{27}	0	C(43)	-1	a_{43}	-1
C(12)	2	a_{12}	1	C(28)	6	a_{28}	-1	C(44)	-1	a_{44}	0
C(13)	-1	a_{13}	1	C(29)	-1	a_{29}	0	C(45)	-8	a_{45}	0
C(14)	6	a_{14}	1	C(30)	-8	a_{30}	0	C(46)	-1	a_{46}	1
C(15)	-8	a_{15}	1	C(31)	-1	a_{31}	1	C(47)	-1	a_{47}	1
C(16)	-1	a_{16}	1	C(32)	-1	a_{32}	1				

Thus in $Q_{105}(x)$ we get -2 as the coefficient of x^7 and of x^{41}.

Note: In computation of C(k) and a_k, actually we don't need to compute all of them, for by one of the properties of the cyclotomic polynomial the coefficients are symmetric to the midterm (in this case the midterm is $a_{24}x^{24}$).

(II) Since $n = 595 = 5 \cdot 7 \cdot 17$, the Euler's ϕ-function

$$\phi(595) = 595 \cdot (1-\frac{1}{5})(1-\frac{1}{7})(1-\frac{1}{17}) = 384$$

so that the degree of $Q_{595}(x)$ is 384

$$Q_{595}(x) = x^{384} + a_1 x^{383} + a_2 x^{382} + \cdots + a_{383} x + 1$$

Employing the exactly same method as in the case of $n = 105$ we can classify all values of k as the following 7 classes. In this case k ranges over 1 through 383.

(1) the multiples of 5; 5, 10, 15, 20, 25, $\cdots$

(2) the multiples of 7; 7, 14, 21, 28, 42, $\cdots$

(3) the multiples of 17; 17, 34, 51, 68, 102, $\cdots$

(4) the multiples of 35; 35, 70, 105, 140, 175, $\cdots$

(5) the multiples of 85; 85, 170, 255, 340.

(6) the multiples of 119; 238, 357.

(7) others; 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, $\cdots$

For each of above classes, the sums of k^{th} powers of the primitive 595^{th} roots of unity are as follows:

(i) The numbers of the class (7) are all relatively prime to 595, that is $(595, k) = 1$ so that we have $C_{595}(k) = \mu(595)$ and since $595 = 5 \cdot 7 \cdot 17$ we get $\mu(595) = -1$, therefore

$$C_{595}(k) = -1$$

(ii) For the class (1) of the multiples of 5, we have $(595, k) = 5$, so that

$$C_{595}(k) = \frac{\mu(\frac{595}{5})\cdot\phi(595)}{\phi(\frac{595}{5})} = \frac{\mu(119)\cdot\phi(595)}{\phi(119)} = \frac{1\times 384}{96} = 4.$$

(iii) For the class (2) of the multiples of 7, we have $(595, k) = 7$, so that

$$C_{595}(k) = \frac{\mu(\frac{595}{7})\cdot\phi(595)}{\phi(\frac{595}{7})} = \frac{\mu(85)\cdot\phi(595)}{\phi(85)} = \frac{1\times 384}{64} = 6.$$

(iv) For the class (3) of the multiples of 17, we have

$$C_{595}(k) = \frac{\mu(\frac{595}{17})\cdot\phi(595)}{\phi(\frac{595}{17})} = \frac{\mu(35)\cdot\phi(595)}{\phi(35)} = \frac{1\times 384}{24} = 16.$$

(v) For the class (4) of the multiples of 35, we have

$$C_{595}(k) = \frac{\mu(\frac{595}{35})\cdot\phi(595)}{\phi(\frac{595}{35})} = \frac{\mu(17)\cdot\phi(595)}{\phi(17)} = \frac{-1\times 384}{16} = -24.$$

(vi) For the class (5) of the multiples of 85, we have

$$C_{595}(k) = \frac{\mu(\frac{595}{85})\cdot\phi(595)}{\phi(\frac{595}{85})} = \frac{\mu(7)\cdot\phi(595)}{\phi(7)} = \frac{-1\times 384}{6} = -64.$$

(vii) For the class (6) of the multiples of 119, we have

$$C_{595}(k) = \frac{\mu(\frac{595}{119}) \cdot \phi(595)}{\phi(\frac{595}{119})} = \frac{\mu(5) \cdot \phi(384)}{\phi(5)} = \frac{-1 \times 384}{4} = -96.$$

Table III. All coefficients and Ramanujan sums of $Q_n(x)$ for $n = 595$.

$C_{595}(k)$		a_k		$C_{595}(i)$		a_k		$C_{595}(k)$		a_k	
C(1)	-1	a_1	1	C(30)	4	a_{30}	0	C(59)	-1	a_{59}	1
C(2)	-1	a_2	1	C(31)	-1	a_{31}	0	C(60)	4	a_{60}	1
C(3)	-1	a_3	1	C(32)	-1	a_{32}	0	C(61)	-1	a_{61}	1
C(4)	-1	a_4	1	C(33)	-1	a_{33}	0	C(62)	-1	a_{62}	1
C(5)	4	a_5	0	C(34)	16	a_{34}	0	C(63)	6	a_{63}	1
C(6)	-1	a_6	0	C(35)	-24	a_{35}	1	C(64)	-1	a_{64}	0
C(7)	6	a_7	-1	C(36)	-1	a_{36}	1	C(65)	4	a_{65}	0
C(8)	-1	a_8	-1	C(37)	-1	a_{37}	1	C(66)	-1	a_{66}	0
C(9)	-1	a_9	-1	C(38)	-1	a_{38}	1	C(67)	-1	a_{67}	0
C(10)	4	a_{10}	-1	C(39)	-1	a_{39}	1	C(68)	16	a_{68}	0
C(11)	-1	a_{11}	-1	C(40)	4	a_{40}	0	C(69)	-1	a_{69}	0
C(12)	-1	a_{12}	0	C(41)	-1	a_{41}	0	C(70)	-24	a_{70}	1
C(13)	-1	a_{13}	0	C(42)	6	a_{42}	-1	C(71)	-1	a_{71}	1
C(14)	6	a_{14}	0	C(43)	-1	a_{43}	-1	C(72)	-1	a_{72}	1
C(15)	4	a_{15}	0	C(44)	-1	a_{44}	-1	C(73)	-1	a_{73}	1
C(16)	-1	a_{16}	0	C(45)	4	a_{45}	-1	C(74)	-1	a_{74}	1
C(17)	16	a_{17}	-1	C(46)	-1	a_{46}	-1	C(75)	4	a_{75}	0
C(18)	-1	a_{18}	-1	C(47)	-1	a_{47}	0	C(76)	-1	a_{76}	0
C(19)	-1	a_{19}	-1	C(48)	-1	a_{48}	0	C(77)	6	a_{77}	-1
C(20)	4	a_{20}	-1	C(49)	6	a_{49}	0	C(78)	-1	a_{78}	-1
C(21)	6	a_{21}	-1	C(50)	4	a_{50}	0	C(79)	-1	a_{79}	-1
C(22)	-1	a_{22}	0	C(51)	16	a_{51}	0	C(80)	4	a_{80}	-1
C(23)	-1	a_{23}	0	C(52)	-1	a_{52}	-1	C(81)	-1	a_{81}	-1
C(24)	-1	a_{24}	1	C(53)	-1	a_{53}	-1	C(82)	-1	a_{82}	0
C(25)	4	a_{25}	1	C(54)	-1	a_{54}	-1	C(83)	-1	a_{83}	0
C(26)	-1	a_{26}	1	C(55)	4	a_{55}	-1	C(84)	6	a_{84}	0
C(27)	-1	a_{27}	1	C(56)	6	a_{56}	-1	C(85)	-64	a_{85}	1
C(28)	6	a_{28}	1	C(57)	-1	a_{57}	0	C(86)	-1	a_{86}	1
C(29)	-1	a_{29}	0	C(58)	-1	a_{58}	0	C(87)	-1	a_{87}	0

Table III (continued)

$C_{595}(k)$		a_k		$C_{595}(k)$		a_k		$C_{595}(k)$		a_k	
C(88)	-1	a_{88}	0	C(119)	-96	a_{119}	1	C(150)	4	a_{150}	-1
C(89)	-1	a_{89}	0	C(120)	4	a_{120}	2	C(151)	-1	a_{151}	-1
C(90)	4	a_{90}	-1	C(121)	-1	a_{121}	2	C(152)	-1	a_{152}	0
C(91)	6	a_{91}	-1	C(122)	-1	a_{122}	1	C(153)	16	a_{153}	0
C(92)	-1	a_{92}	-1	C(123)	-1	a_{123}	1	C(154)	6	a_{154}	1
C(93)	-1	a_{93}	-1	C(124)	-1	a_{124}	0	C(155)	4	a_{155}	2
C(94)	-1	a_{94}	0	C(125)	4	a_{125}	-1	C(156)	-1	a_{156}	2
C(95)	4	a_{95}	0	C(126)	6	a_{126}	-2	C(157)	-1	a_{157}	1
C(96)	-1	a_{96}	0	C(127)	-1	a_{127}	-2	C(158)	-1	a_{158}	0
C(97)	-1	a_{97}	1	C(128)	-1	a_{128}	-2	C(159)	-1	a_{159}	0
C(98)	6	a_{98}	1	C(129)	-1	a_{129}	-1	C(160)	4	a_{160}	-1
C(99)	-1	a_{99}	0	C(130)	4	a_{130}	-1	C(161)	6	a_{161}	-2
C(100)	4	a_{100}	0	C(131)	-1	a_{131}	0	C(162)	-1	a_{162}	-2
C(101)	-1	a_{101}	0	C(132)	-1	a_{132}	1	C(163)	-1	a_{163}	-2
C(102)	16	a_{102}	-1	C(133)	6	a_{133}	1	C(164)	-1	a_{164}	-1
C(103)	-1	a_{103}	-1	C(134)	-1	a_{134}	0	C(165)	4	a_{165}	-1
C(104)	-1	a_{104}	-1	C(135)	4	a_{135}	0	C(166)	-1	a_{166}	0
C(105)	-24	a_{105}	0	C(136)	16	a_{136}	-1	C(167)	-1	a_{167}	1
C(106)	-1	a_{106}	0	C(137)	-1	a_{137}	-2	C(168)	6	a_{168}	1
C(107)	-1	a_{107}	1	C(138)	-1	a_{138}	-2	C(169)	-1	a_{169}	0
C(108)	-1	a_{108}	1	C(139)	-1	a_{139}	-2	C(170)	-64	a_{170}	1
C(109)	-1	a_{109}	2	C(140)	-24	a_{140}	-1	C(171)	-1	a_{171}	0
C(110)	4	a_{110}	1	C(141)	-1	a_{141}	0	C(172)	-1	a_{172}	-1
C(111)	-1	a_{111}	1	C(142)	-1	a_{142}	1	C(173)	-1	a_{173}	-1
C(112)	6	a_{112}	0	C(143)	-1	a_{143}	2	C(174)	-1	a_{174}	-1
C(113)	-1	a_{113}	0	C(144)	-1	a_{144}	3	C(175)	-24	a_{175}	-1
C(114)	-1	a_{114}	-1	C(145)	4	a_{145}	2	C(176)	-1	a_{176}	0
C(115)	4	a_{115}	-1	C(146)	-1	a_{146}	2	C(177)	-1	a_{177}	0
C(116)	-1	a_{116}	-1	C(147)	6	a_{147}	1	C(178)	-1	a_{178}	1
C(117)	-1	a_{117}	0	C(148)	-1	a_{148}	0	C(179)	-1	a_{179}	2
C(118)	-1	a_{118}	0	C(149)	-1	a_{149}	-1	C(180)	4	a_{180}	1

Table III (continued)

$C_{595}(k)$		a_k		$C_{595}(k)$		a_k		$C_{595}(k)$		a_k	
C(181)	-1	a_{181}	1	C(212)	-1	a_{212}	-1	C(243)	-1	a_{243}	0
C(182)	6	a_{182}	1	C(213)	-1	a_{213}	0	C(244)	-1	a_{244}	-1
C(183)	-1	a_{183}	0	C(214)	-1	a_{214}	1	C(245)	-24	a_{245}	-2
C(184)	-1	a_{184}	-1	C(215)	4	a_{215}	0	C(246)	-1	a_{246}	-2
C(185)	4	a_{185}	-1	C(216)	-1	a_{216}	1	C(247)	-1	a_{247}	-2
C(186)	-1	a_{186}	-1	C(217)	6	a_{217}	1	C(248)	-1	a_{248}	-1
C(187)	16	a_{187}	-1	C(218)	-1	a_{218}	0	C(249)	-1	a_{249}	0
C(188)	-1	a_{188}	-1	C(219)	-1	a_{219}	-1	C(250)	4	a_{250}	0
C(189)	6	a_{189}	0	C(220)	4	a_{220}	-1	C(251)	-1	a_{251}	1
C(190)	4	a_{190}	1	C(221)	16	a_{221}	-2	C(252)	6	a_{252}	1
C(191)	-1	a_{191}	1	C(222)	-1	a_{222}	-2	C(253)	-1	a_{253}	0
C(192)	-1	a_{192}	1	C(223)	-1	a_{223}	-2	C(254)	-1	a_{254}	-1
C(193)	-1	a_{193}	1	C(224)	6	a_{224}	-1	C(255)	-64	a_{255}	-1
C(194)	-1	a_{194}	1	C(225)	4	a_{225}	0	C(256)	-1	a_{256}	-2
C(195)	4	a_{195}	0	C(226)	-1	a_{226}	0	C(257)	-1	a_{257}	-2
C(196)	6	a_{196}	-1	C(227)	-1	a_{227}	1	C(258)	-1	a_{258}	-2
C(197)	-1	a_{197}	-1	C(228)	-1	a_{228}	2	C(259)	6	a_{259}	-1
C(198)	-1	a_{198}	-1	C(229)	-1	a_{229}	2	C(260)	4	a_{260}	0
C(199)	-1	a_{199}	-1	C(230)	4	a_{230}	1	C(261)	-1	a_{261}	1
C(200)	4	a_{200}	-1	C(231)	6	a_{231}	0	C(262)	-1	a_{262}	1
C(201)	-1	a_{201}	0	C(232)	-1	a_{232}	0	C(263)	-1	a_{263}	2
C(202)	-1	a_{202}	1	C(233)	-1	a_{233}	-1	C(264)	-1	a_{264}	2
C(203)	6	a_{203}	1	C(234)	-1	a_{234}	-1	C(265)	4	a_{265}	1
C(204)	16	a_{204}	1	C(235)	4	a_{235}	-1	C(266)	6	a_{266}	0
C(205)	4	a_{205}	2	C(236)	-1	a_{236}	0	C(267)	-1	a_{267}	0
C(206)	-1	a_{206}	1	C(237)	-1	a_{237}	1	C(268)	-1	a_{268}	-1
C(207)	-1	a_{207}	0	C(238)	-96	a_{238}	2	C(269)	-1	a_{269}	-1
C(208)	-1	a_{208}	0	C(239)	-1	a_{239}	2	C(270)	4	a_{270}	-1
C(209)	-1	a_{209}	-1	C(240)	4	a_{240}	3	C(271)	-1	a_{271}	0
C(210)	24	a_{210}	-1	C(241)	-1	a_{241}	2	C(272)	16	a_{272}	0
C(211)	-1	a_{211}	-1	C(242)	-1	a_{242}	1	C(273)	6	a_{273}	1

Table III (continued)

$C_{595}(k)$		a_k		$C_{595}(k)$		a_k		$C_{595}(k)$		a_k	
C(274)	-1	a_{274}	1	C(305)	4	a_{305}	-1	C(336)	6	a_{336}	0
C(275)	4	a_{275}	2	C(306)	16	a_{306}	-1	C(337)	-1	a_{337}	0
C(276)	-1	a_{276}	1	C(307)	-1	a_{307}	-1	C(338)	-1	a_{338}	-1
C(277)	-1	a_{277}	1	C(308)	6	a_{308}	0	C(339)	-1	a_{339}	-1
C(278)	-1	a_{278}	0	C(309)	-1	a_{309}	0	C(340)	-64	a_{340}	-1
C(279)	-1	a_{279}	0	C(310)	4	a_{310}	1	C(341)	-1	a_{341}	-1
C(280)	-24	a_{280}	-1	C(311)	-1	a_{311}	1	C(342)	-1	a_{342}	-1
C(281)	-1	a_{281}	-1	C(312)	-1	a_{312}	1	C(343)	6	a_{343}	0
C(282)	-1	a_{282}	-1	C(313)	-1	a_{313}	1	C(344)	-1	a_{344}	0
C(283)	-1	a_{283}	0	C(314)	-1	a_{314}	1	C(345)	4	a_{345}	1
C(284)	-1	a_{284}	0	C(315)	-24	a_{315}	0	C(346)	-1	a_{346}	1
C(285)	4	a_{285}	0	C(316)	-1	a_{316}	0	C(347)	-1	a_{347}	1
C(286)	-1	a_{286}	1	C(317)	-1	a_{317}	0	C(348)	-1	a_{348}	1
C(287)	6	a_{287}	1	C(318)	-1	a_{318}	0	C(349)	-1	a_{349}	1
C(288)	-1	a_{288}	0	C(319)	-1	a_{319}	0	C(350)	-24	a_{350}	0
C(289)	16	a_{289}	0	C(320)	4	a_{320}	0	C(351)	-1	a_{351}	0
C(290)	4	a_{290}	0	C(321)	-1	a_{321}	1	C(352)	-1	a_{352}	0
C(291)	-1	a_{291}	-1	C(322)	6	a_{322}	1	C(353)	-1	a_{353}	0
C(292)	-1	a_{292}	-1	C(323)	16	a_{323}	1	C(354)	-1	a_{354}	0
C(293)	-1	a_{293}	-1	C(324)	-1	a_{324}	1	C(355)	4	a_{355}	0
C(294)	6	a_{294}	-1	C(325)	4	a_{325}	1	C(356)	-1	a_{356}	1
C(295)	4	a_{295}	0	C(326)	-1	a_{326}	0	C(357)	-96	a_{357}	1
C(296)	-1	a_{296}	0	C(327)	-1	a_{327}	0	C(358)	-1	a_{358}	1
C(297)	-1	a_{297}	0	C(328)	-1	a_{328}	-1	C(359)	-1	a_{359}	1
C(298)	-1	a_{298}	1	C(329)	6	a_{329}	-1	C(360)	4	a_{360}	1
C(299)	-1	a_{299}	1	C(330)	4	a_{330}	-1	C(361)	-1	a_{361}	0
C(300)	4	a_{300}	0	C(331)	-1	a_{331}	-1	C(362)	-1	a_{362}	0
C(301)	6	a_{301}	0	C(332)	-1	a_{332}	-1	C(363)	-1	a_{363}	-1
C(302)	-1	a_{302}	0	C(333)	-1	a_{333}	0	C(364)	6	a_{364}	-1
C(303)	-1	a_{303}	-1	C(334)	-1	a_{334}	0	C(365)	4	a_{365}	-1
C(304)	-1	a_{304}	-1	C(335)	4	a_{335}	0	C(366)	-1	a_{366}	-1

Table III (continued)

$C_{595}(k)$		a_k		$C_{595}(k)$		a_k		$C_{595}(k)$		a_k	
C(367)	-1	a_{367}	-1	C(373)	-1	a_{373}	-1	C(379)	-1	a_{379}	0
C(368)	-1	a_{368}	0	C(374)	16	a_{374}	-1	C(380)	4	a_{380}	1
C(369)	-1	a_{369}	0	C(375)	4	a_{375}	-1	C(381)	-1	a_{381}	1
C(370)	4	a_{370}	0	C(376)	-1	a_{376}	-1	C(382)	-1	a_{382}	1
C(371)	6	a_{371}	0	C(377)	-1	a_{377}	-1	C(383)	-1	a_{383}	1
C(372)	-1	a_{372}	0	C(378)	6	a_{378}	0				

E. Lehmer says that the coefficient of x^h where $h = (p-3)(qr+1)/2$ is $(p-1)/2$. In this case $h = 120$ so that the coefficient of x^{120} is 2 and this coincides with the result obtained directly from the calculation method, that is, the coefficient of x^{120} is $a_{264} = 2$.

Since the coefficients are symmetric to the midterm the coefficient of x^{264} is also equal to 2.

We can also see that there exist other "large" coefficients and "larger" coefficients (in absolute value) in addition to the coefficient a_h in Lehmer's case.

We observe that adjacent coefficients in Tables II and III do not differ by more than 1 in absolute value. It would be of interest to prove this in general or find a counterexample but this is beyond the scope of the paper.

BIBLIOGRAPHY

1. Bang, A. S. Om Ligningen $\phi_n(x) = 0$. Nyt Tidsskrift for Mathematik, ser. B, 6:6-12. 1895.

2. Bateman, P. T. Note on the coefficients of the cyclotomic polynomial. Bulletin of the American Mathematical Society 52:179-184. 1946.

3. Beiter, Sister M. The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$. American Mathematical Monthly 71:769-770. 1964.

4. Carlitz, L. The number of terms in the cyclotomic polynomial $Q_{pq}(x)$. American Mathematical Monthly 73:979-981. 1966.

5. Eatön, J. E. A formula for the coefficients of the cyclotomic polynomial. Bulletin of the American Mathematical Society 45:178-186. 1939.

6. Erdős, P. On the coefficients of the cyclotomic polynomial. Bulletin of the American Mathematical Society 52:179-184. 1946.

7. Gagliardo, E. Le funzioni simmetriche semplici delle radici n-esime primitive dell' unità. Bolletino della unione matematica Italiano 3:268-273. 1953.

8. Herstein, I. N. Topics in algebra. Waltham, Mass., Blaisdell, 1964. 342 p.

9. Hőlder, Ő. Zur Theorie der Kreisteilungsgleichung $k_m(x)=0$. Prace Matematyczno-Fizyczne (Warsaw) 43:13-23. 1936.

10. Jacőbson, N. Lectures in abstract algebra. vol. 3. Princeton, N. J., Van Nostrand, 1964. 323 p.

11. Kazandzidis, G. S. On the cyclotomic polynomial; coefficients. Bulletin de la Societe Mathematique de Gréce (Athens), new ser., 4(1):1-11. 1963.

12. Lehmer, E. On the magnitude of the coefficients of the cyclotomic polynomial. Bulletin of the American Mathematical Society 42:389-392. 1936.

13. Niven, I. and H. S. Zuckerman. An introduction to the theory of numbers. New York, Wiley, 1960. 250 p.

14. Perron, O. Algebra. vol. 1. Die Grundlagen. Berlin, Walter de Gruyter, 1932. 300 p.

15. Rademacher, H. Lecture on elementary number theory. Waltham, Mass., Blaisdell, 1964. 146 p.

16. van der Waerden, B. L. Modern algebra, tr. by Fred Blum. vol. 1. New York, Frederik Ungar, 1953. 264 p.